KRYPTOGRAFIA

Możliwość przekształcania danych w taki sposób, aby były dostępne tylko dla uprawnionych osób, to tylko jedna z wielu wartościowych usług wykonywanych przez technologię powszechnie zwaną szyfrowaniem. Ta technologia pojawiła się w innych sekcjach ale niektórzy czytelnicy mogą nie znać jej zasad i źródeł. Celem tej części jest wyjaśnienie podstawowych zagadnień związanych z technologią szyfrowania i opisanie jej zastosowania w takich obszarach, jak szyfrowanie plików, szyfrowanie wiadomości, uwierzytelnianie i bezpieczne transakcje internetowe. To nie jest teoretyczny lub naukowy traktat o szyfrowaniu, ale praktyczny przewodnik dla tych, którzy muszą stosować szyfrowanie w kontekście bezpieczeństwa komputerowego. Organizacje na całym świecie coraz częściej polegają na kryptografii, aby się komunikować bezpiecznie i bezpiecznie przechowywać informacje. Zazwyczaj algorytmy używane przez organizacje Departamentu Obrony (DoD) są stosowane i utrzymywane przez wiele lat. Na przykład standard szyfrowania danych (DES) był używany w jakiejś formie przez ponad 20 lat. Ta część to krótki przegląd kryptografii i jej praktyczne zastosowanie do potrzeb zwykłych użytkowników biznesowych, w odróżnieniu od potrzeb agencji rządowych o wysokim poziomie bezpieczeństwa. Dokładne zbadanie matematyki, które jest podstawą tych tematów, wykracza poza zakres tego rozdziału, ale proponujemy odczyty na dalsze badanie.

TERMINOLOGIA

Ta lista podstawowych terminów będzie pomocna dla czytelników, ponieważ będą oni kontynuować tę część:

Algorytm - skończona lista dobrze zdefiniowanych instrukcji do wykonania zadania, które z uwagi na stan początkowy zakończy się w określonym stanie końcowym.

Szyfr - podstawowy algorytm używany do szyfrowania danych. Szyfr przekształca zwykły tekst w zaszyfrowany tekst, który nie jest odwracalny bez klucza. Tekst zaszyfrowanego tekstu w postaci zaszyfrowanej, w przeciwieństwie do zwykłego tekstu. W całym tym rozdziale pokazujemy tekst w UPPERCASE.

Kody - lista równoważników (słownik kodów) umożliwia zamianę znaczącego tekstu na słowa, wyrażenia lub zdania w niewinnej wiadomości; na przykład: "Kupię kwiaty dla Mamy jutro na jej przyjęcie o 19:00" może zostać odkodowany, aby oznaczać "Rozpocznij atak na statek macierzysty w przyszłym tygodniu w niedzielę".

Deszyfrowanie - proces pobierania tekstu jawnego z zaszyfrowanego tekstu.

Szyfrowanie - aby zmienić zwykły tekst za pomocą tajnego kodu, tak aby był niezrozumiały dla nieautoryzowanych stron.

Klucz - słowo lub system do rozwiązywania szyfrów lub kodów.

Jawny tekst - oryginalna wiadomość do zakodowania lub zaszyfrowania. W całym tekście wyświetlamy zwykły tekst małymi literami.

Nauka o kryptologii (czasami skracana jako krypto) to nauka o bezpiecznej komunikacji, utworzona z greckich słów (kryptos), co oznacza "ukryte" i (logos), "słowo". Dokładniej, jest to badanie dwa odrębne, ale bardzo powiązane ze sobą obszary badań: kryptografia i kryptoanaliza. Kryptografia jest to :

Nauka o kodowaniu i dekodowaniu wiadomości, aby zapewnić bezpieczeństwo tych wiadomości. Kryptoanaliza jest sztuką i nauką łamania kodów, dekodowania sekretów, łamania schematów

uwierzytelniania i ogólnie łamania protokołów kryptograficznych, wszystko bez znajomości tajnego klucza.

Systemy do szyfrowania informacji określane są jako kryptosystemy. Systemy do szyfrowania informacji mogą być również nazywane systemami szyfrującymi, z szyfru, co oznacza "zero" lub "pusty" (słowo zakorzenione w sifr arabskim). Terminy używające szyfrów i krypto są zamienne, a niektórzy autorzy wolą szyfr, aby uniknąć religijnych i kulturowych konotacji krypty, słowo o tym samym źródle co "szyfrowanie". W ten sposób szyfrowanie może być określane jako szyfrowanie, odszyfrowywanie zwane rozszyfrowaniem, i tak dalej. Najbardziej oczywistym zastosowaniem szyfrowania jest przeszukanie zawartości pliku lub wiadomości, używając jakiejś formy wspólnego sekretu jako klucza. Bez klucza zaszyfrowane dane pozostają ukryte i nie można ich rozszyfrować ani odszyfrować. Całkowita liczba możliwych kluczy dla algorytmu szyfrowania nazywana jest keyspace. Keyspace jest funkcją funkcji długości klucza i liczbą możliwych wartości w każdej pozycji klucza. Dla długości klucza n pozycji, przy czym każda pozycja ma v możliwych wartości, wtedy keyspace dla tego klucza będzie vn. Na przykład, w trzech pozycjach i dwóch wartościach na pozycję (np. 0 lub 1), możliwe klucze będą wynosić 000, 001, 010, 011, 100, 101, 110 i 111 dla całkowitej przestrzeni kluczy wynoszącej 8

ROLA KRPTOGRAFII

Główną rolą kryptografii w bezpieczeństwie komputerów jest zapewnienie poufności danych. Ale kryptografia może obsługiwać inne filary bezpieczeństwa komputerowego, takie jak integralność i autentyczność. Ta sekcja omawia różne role kryptografii

POUFNOŚĆ

Rola szyfrowania w ochronie poufności można dostrzec w klasycznej definicji szyfrowania: "Szyfrowanie to specjalne obliczenia, które działają na wiadomościach, przekształcając je w reprezentację, która jest bez znaczenia dla wszystkich stron innych niż zamierzony odbiorca." Znaczna część literatury w sprawie kryptografii omawia technologię pod względem zapewnienia poufności wiadomości, ale jest to funkcjonalnie równoważne ochronie poufności danych. Użycie terminu "wiadomość" odzwierciedla tradycyjne zastosowanie, jakim została poddana kryptografia, zarówno przed, jak i po pojawieniu się komputerów. Na przykład, Juliusz Cezar zaszyfrował wiadomości do Cicero 2000 lat temu, podczas gdy dzisiaj wiadomości pomiędzy przeglądarką internetową a serwerem sieciowym są szyfrowane podczas przeprowadzania "bezpiecznej" transakcji. Stosując kryptografię do ochrony komputera, czasem należy zastąpić termin "pliki" terminem "wiadomości". Na przykład programy do szyfrowania dysku twardego chronią pliki danych przechowywane na dysku twardym. Pliki danych mają jednak postać wiadomości przesyłanych z jednego komputera do drugiego, przez sieć, Internet lub linie telefoniczne. Praktycznie rzecz biorąc, dane przesyłane w ten sposób są narażone na inny zestaw zagrożeń od tych, które zagrażają danych przechowywanych na komputerze w biurze. W związku z tym użycie szyfrowania w celu uczynienia plików bezużytecznymi dla kogokolwiek innego niż uprawniony użytkownik jest istotne zarówno dla plików w tranzycie, jak i dla tych, które znajdują się na serwerze lub komputerze autonomicznym, szczególnie gdy jest to laptop, notebook lub inny komputer. PDA.

UCZCIWOŚĆ

W drugiej połowie ubiegłego wieku, po pojawieniu się programowalnych systemów komputerowych, zdolność kryptografii do transformacji danych została zastosowana na wiele nowych i interesujących sposobów. Jak zobaczymy za chwilę, wiele technik kryptograficznych wykorzystuje wiele matematycznych obliczeń. Zdolność komputerów do wykonywania wielu obliczeń w krótkim czasie znacznie zwiększyła użyteczność kryptografii, a także zainspirowała rozwój coraz silniejszych systemów

szyfrowania. Zachowanie integralności danych jest często tak samo ważne, jak zachowanie poufności. Pisząc czeki, ludzie starają się udaremnić zmianę odbiorcy lub kwotę. W niektórych przypadkach integralność jest ważniejsza niż poufność. Zmiana treści komunikatu prasowego firmy, gdy przechodzi z firmy do prasy, może mieć poważne konsekwencje. Nie tylko ludzkie działania zagrażają integralności danych; uszkodzenia mechaniczne i błędy logiczne mogą również zmieniać dane. Istotne jest, aby wykryć takie zmiany, jak to omówiono wcześniej, gdy zaobserwowano, że "wszystkie ruchy danych i tłumaczenia zwiększają prawdopodobieństwo wystąpienia błędu wewnętrznego, dlatego też kontrole parzystości i testy ważności stały się niezbędne." Rozdział ten obejmował rola bitów parzystości do wykrywania błędów, funkcja kontroli nadmiarowości oraz wykorzystanie sum kontrolnych w celu zapewnienia możliwości wykrywania modyfikacji. Typ kryptograficznego skrótu lub sumy kontrolnej o nazwie Kod uwierzytelniania wiadomości (MAC) może chronić przed zamierzonymi, ale nieautoryzowanymi modyfikacjami danych, jak również przed przypadkową modyfikacją. MAC jest obliczany przez zastosowanie algorytmu kryptograficznego i tajnej wartości zwanej kluczem do danych. Dane są później weryfikowane przez zastosowanie algorytmu kryptograficznego i tego samego tajnego klucza do danych w celu wytworzenia innego adresu MAC; ten MAC jest następnie porównywany z początkowym MAC. Jeśli oba MAC są równe, dane są uważane za autentyczne. W przeciwnym razie zakłada się nieautoryzowaną modyfikację (każda strona próbująca zmodyfikować dane bez znajomości klucza nie będzie wiedziała, jak obliczyć odpowiedni MAC odpowiadający zmienionym danym).

UWIERZYTELNIENIE

W kontekście bezpieczeństwa komputerowego uwierzytelnianie to możliwość potwierdzenia tożsamości użytkowników. Na przykład wiele komputerów prosi teraz użytkowników o zalogowanie się przed uzyskaniem dostępu do danych. Żądając nazwy użytkownika i hasła, systemy próbują upewnić się, że tylko autentyczni użytkownicy mogą uzyskać dostęp. Jednak ta forma uwierzytelniania jest ograniczona - zapewnia jedynie, że osoba logująca się to osoba znająca poprawną nazwę użytkownika i parę haseł. Kryptografia odgrywa bardzo ważną rolę w wysiłkach na rzecz zapewnienia silniejszego uwierzytelniania, od szyfrowania dane haseł do tworzenia i weryfikacji identyfikatorów elektronicznych, takich jak podpis cyfrowy. Zostaną one opisane bardziej szczegółowo w dalszej części tego rozdziału, wraz z różnicami między kluczem publicznym a kryptografią klucza prywatnego, z których oba mogą być używane w tych schematach. Za pomocą systemu klucza publicznego dokumenty w systemie komputerowym można elektronicznie podpisywać, stosując do dokumentu klucz prywatny inicjatora. Wynikowy podpis cyfrowy i dokument mogą być następnie przechowywane lub przesyłane. Podpis można zweryfikować przy użyciu klucza publicznego nadawcy. Jeśli podpis weryfikuje prawidłowo, odbiorca ma pewność, że dokument został podpisany przy użyciu klucza prywatnego nadawcy i że wiadomość nie została zmieniona po jej podpisaniu. Ponieważ klucze prywatne są znane tylko ich właścicielowi, możliwe jest również sprawdzenie źródła informacji na rzecz strony trzeciej.

NIEZAPRZECZALNOŚĆ

Aspektem bezpieczeństwa komputerowego, które znacznie wzrosło ze względu na wzrost liczby transakcji w sieci, jest nieodrzucanie. Na przykład, jeśli ktoś złoży elektroniczne zamówienie na sprzedaż akcji, które później zwiększa wartość, ważne jest, aby udowodnić, że zamówienie zdecydowanie pochodzi od osoby, która go złożyła. Możliwe dzięki kryptografii z kluczem publicznym, nieodparcie pomaga zapewnić, że strony komunikacji nie mogą zaprzeczyć, że uczestniczyły w całości lub części komunikacji.

OGRANICZENIE

Jedną z funkcji, których nie może wypełnić kryptografia, jest obrona przed zniszczeniem danych. Chociaż szyfrowanie nie zapewnia dostępności, stanowi bardzo cenną dodatkową linię obrony dla informacji komputerowych, gdy dodaje się ją do fizycznego bezpieczeństwa, kontroli dostępu do systemu i bezpiecznych kanałów komunikacji. W rzeczywistości, gdy komputery są mobilne lub dane są komunikowane za pośrednictwem niezabezpieczonych kanałów, szyfrowanie może być główną linią obrony. Jednak nawet jeśli zastosowana kryptografia może zapewnić użytkownikom komputerów poziomy bezpieczeństwa, których nie da się pokonać bez specjalistycznej wiedzy i wydajnych komputerów, szyfrowanie danych nie powinno być uważane za alternatywę lub substytut kontroli dostępu do systemu. Według Seberry'ego i Pieprzyka, rolą kryptografii jest ochrona "informacji, do których możliwy jest nielegalny dostęp i gdzie inne środki ochronne są nieskuteczne". Kontrola dostępu do plików za pomocą szyfrowania powinna stanowić trzecią barierę po kontroli dostępu do witryny i systemu, jeśli z innego powodu niż to, że same systemy szyfrowania w niewielkim stopniu uniemożliwiają usuwanie plików.

PODSTAWOWA KRYPTOGRAFIA

Celem kryptografii jest opracowanie systemów, które mogą szyfrować zwykły tekst w zaszyfrowanym tekście, który jest nieodróżnialny od czysto losowego zbioru danych. Oznacza to, że wszystkie możliwe odszyfrowane wersje danych, z wyjątkiem jednej, będą beznadziejnie niejednoznaczne, a żadna z nich nie będzie bardziej poprawna niż jakiekolwiek inne. Jednym z najprostszych sposobów tworzenia zaszyfrowanego tekstu jest przedstawienie każdego znaku lub słowa w zwykłym tekście za pomocą innego znaku lub słowa w zaszyfrowanym tekście, tak, że nie ma natychmiastowo widocznego związku między dwiema wersjami tego samego tekstu.

WCZESNE SZYFRY

Uważa się, że najwcześniejszy tekst wykazujący podstawowy atrybut kryptografii, po niewielkiej modyfikacji tekstu, wystąpił w Egipcie prawie 4000 lat temu. Skryba użył wielu nietypowych symboli, aby zmylić lub zasłonić znaczenie hieroglificznych napisów na grobie szlachcica o nazwisku Khnumhotep II. Uważa się również, że pierwszym skutecznym wojskowym użyciem kryptografii był prosty szyld transpozycyjny Spartan, który "Już w 400 rpne używano urządzenia szyfrującego, zwanego" scytale "do tajnej komunikacji między dowódcami wojskowymi." Scytale było cylindrycznym lub stożkowym drążkiem z cienkim pasem ze skóry lub pergaminu owiniętego spiralnie. Wiadomość do ukrycia była napisana wzdłużnie bez pustych miejsc. Po rozplątaniu pergamin wydawał się nie zawierać nic prócz przypadkowych liter. Aby odczytać pergamin, odbiorca musiał mieć patyk o dokładnie takich samych wymiarach jak nadawca. Rozmieszczenie odpowiednich kodów dekodujących miało miejsce zanim dowódcy wojskowi odeszli na pole. Na przykład określona kombinacja sztyftu i paska może umożliwić tekst jawny:

atheniantroopswithionaysmarchofromereadynow

zostać podzielone na sześć rzędów ośmiu liter, które zostaną zapisane w zwiniętym ciągu aby rozebrać w ten sposób:

ateński

troopswi

rozcieńczony

aysmarch

ofromebe

teraz gotów

Wiadomość może pojawić się w scytale. Odczytanie nieopakowanego paska bez patyka spowoduje wygenerowanie tego zaszyfrowanego tekstu (pokazanego wielkimi literami):

ATTAORTRHYFEHOISREEONMODNPOAMYISNRENAWECBONIDHEW

"Pierwsze potwierdzone użycie [szyfru zastępczego] w sprawach wojskowych pochodzi od Rzymian." W tym czasie Juliusz Cezar zakodował wszystkie swoje wiadomości, zastępując każdą literę literą trzy miejsca dalej. Na przykład litera może stać się literą d, litera b stanie się literą e, i tak dalej. Teraz nazywany Szyfrem Cezara, ten schemat jest najlepiej znany ze wszystkich algorytmów monoalchetycznych. Rozważ szyfr cezara zilustrowany w następnym porównaniu używając nowoczesnego alfabetu angielskiego, z literami alfabetu po prostu przesuniętymi o trzy miejsca.

Plaintext: abcdefghijklmnopqrstuvwxyz

Tekst zaszyfrowany: DEFGHIJKLMNOPQRSTUVWXYZABC

Aby zaszyfrować wiadomość, nadawca znajduje każdą literę wiadomości w alfabecie zwykłego tekstu i używa litery pod nim w alfabecie tekstu zaszyfrowanego. Tak więc jasny komunikat:

Czysty tekst: strzeż się przemarszów marszu

jest przekształcany w zaszyfrowaną wiadomość:

Tekst zaszyfrowany: EHZDUH WKH LGHV RI PDUFK

Ten rodzaj szyfrowania jest znany jako szyfr zastępczy. Chociaż szyfr Cezara jest stosunkowo prosty, szyfry zastępcze mogą być bardzo potężne. Większość przykładów szyfru Caesara przesuwa alfabet o trzy miejsca, jak pokazano, tak aby linia tekstu zaszyfrowanego zaczynała się od d, ale niektórzy autorzy sugerują, że Cezar mógł użyć innych liczb, więc termin "Szyfr Cezara" jest używany dla wszystkich szyfrów zgodnych z tym algorytmem (algorytm będący formułą lub receptą na rozwiązanie problemu). Ten poziom szyfrowania może wydawać się prymitywny, ale jest to ważny punkt wyjścia dla wielu następnych. Na przykład, jednym ze sposobów wizualizacji szyfru Cezara jest para pierścieni, jeden w drugim

Oba okręgi zawierają litery alfabetu. Jeśli jeden jest obrócony względem drugiego, wynikiem jest koło szyfrujące, coś dobrze przystosowanego do automatyzacji. W końcu tak się stało, najpierw mechanicznie, potem elektrycznie, a dziś cyfrowo. Automatyzacja ułatwia powtórzenie, a wiadomości zaszyfrowane za pomocą szyfru zastępczego mogą być trudniejsze do rozszyfrowania, jeśli zastosuje się wiele różnych podstawień. Tak więc koło kodu dostało miejsce w pieczęcie NSA, agencji rządowej USA, która ma największy wpływ na rozwój szyfrowania.

BARDZIEJ TAJEMNICZA TERMINOLOGIA

Klucz lub hasło do szyfru Cezara przedstawione w ostatniej sekcji to liczba miejsc, w których alfabet został przesunięty, w tym przypadku trzy. Ponieważ klucz ten musi pozostać prywatny, aby wiadomość pozostała chroniona, musi zostać dostarczona do odbiorcy, aby wiadomość została zdekodowana lub odszyfrowana z powrotem do zwykłego tekstu. Dlatego szyfr cezara jest opisany jako algorytm klucza prywatnego, a także symetryczny algorytm szyfrowania, przy użyciu tego samego klucza prywatnego, który jest używany do szyfrowania i odszyfrowywania wiadomości. Algorytmy tego typu mogą zostać pokonane przez kogoś, kto ma klucz, zaszyfrowaną wiadomość i znajomość użytego algorytmu. Może to brzmieć jak stwierdzenie tego, co oczywiste; jednak, jak zobaczymy w dalszej części tego rozdziału, istnieją algorytmy szyfrowania, które wykorzystują klucze, które można jawnie wymieniać bez

udostępniania danych zaszyfrowanych. Znajomość zastosowanego algorytmu często można uzyskać lub poddać inżynierii wstecznej analizie jego wydajności. Innym pozornie oczywistym faktem jest to, że gdy używa się klucza prywatnego, aby osiągnąć poufność, jeden problem zostaje zamieniony na inny. Problem wymiany wiadomości przy zachowaniu zawartości od niezamierzonych odbiorców zostaje zastąpiony przez problem wymiany kluczy między nadawcą a odbiorcą bez ujawniania kluczy. Ten nowy problem jest znany jako problem wymiany klucza. Problem z wymianą kluczy zostanie bardziej szczegółowo zbadany później.

PODSTAWOWA KRYPTOANALIZA

"Pierwszymi ludźmi, którzy zrozumieli wyraźnie zasady kryptografii i wyjaśnienia początków kryptoanalizy, byli Arabowie." Do piętnastego wieku odkryli technikę analizy rozkładu częstotliwości liter i pomyślnie odszyfrowali grecką wiadomość w drodze do Cesarz bizantyjski. W 1492 roku człowiek znany jako al-Kalka-shandi opisał tę technikę w encyklopedii. Opisał także kilka technik kryptograficznych, w tym szyfru zastępczego i transpozycji. Wracając do szyfru Caesara, zastanów się, jak ten kod mógł zostać złamany przy pomocy nauki kryptoanalizy. Podczas badania przez pewien czas ten konkretny kod jest dość przejrzysty. Jak tylko kilka liter zostanie poprawnie zidentyfikowanych, reszta zostanie wprowadzona. Na przykład, ponieważ "the" jest najczęściej używanym trzyliterowym słowem w języku angielskim, testowanie "XLI" względem "the" ujawnia, że każda litera tekstu jawnego ma ustalony związek z zaszyfrowanym tekstem: przesunięcie trzech w prawo. Jeśli ta różnica zostanie zastosowana do reszty komunikatu, wynikiem jest fragment tekstu jawnego, który jest zrozumiały, a zatem zakłada się, że jest poprawnym rozwiązaniem problemu. Jednak nawet w tym prostym przykładzie działa szereg wyrafinowanych procesów i założeń; zasługują na większą uwagę, zanim przyjrzą się bardziej skomplikowanym kodeksom. Po pierwsze, test "the" przeciwko "XLI" zakłada, że tekst jawny jest angielski i że atakujący ma szczegółową wiedzę o tym języku, na przykład częstotliwość niektórych słów. Po drugie, zakłada się, że zaszyfrowany tekst podąża za tekstem jawnym pod względem słów. Zazwyczaj tak nie jest. Tekst zaszyfrowany jest zwykle pisany blokami liter o jednakowej długości, aby je dalej ukryć, jak w:

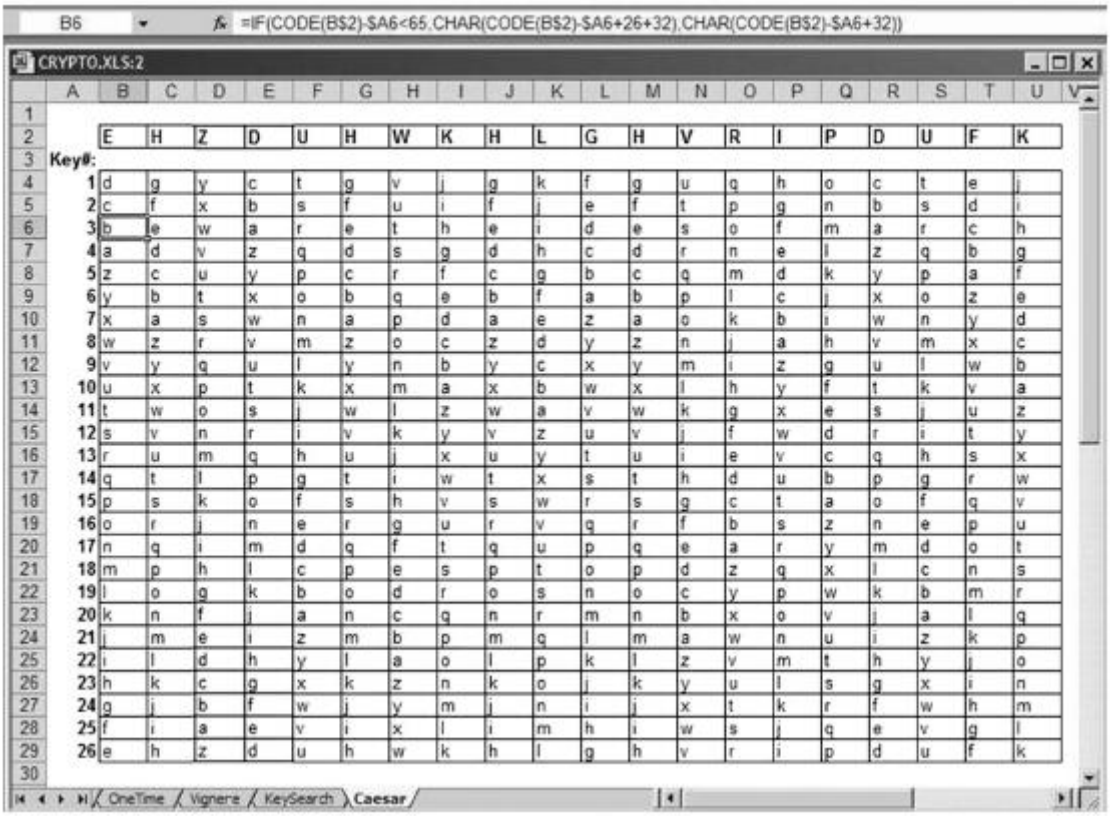
Tekst zaszyfrowany: EHZDU HWKHL GHVRI PDUFK

Gdy odbiorca wiadomości odszyfrowuje go, wynik, choć nie jest dokładnie łatwy do odczytania, jest jednak całkowicie zrozumiały:

Plaintext: bewar ethei desof march Zwróć także uwagę na konwencję ignorowania przypadku pojedynczych liter i umieszczania całego tekstu jawnego małymi literami, podczas gdy cały tekst zaszyfrowany jest wielkimi literami.

KRYPTOANALIZA BRUTE FORCE

Następną rzeczą, na którą warto zwrócić uwagę na szyfr Cezara, jest to, że używając alfabetu angielskiego istnieje 26 możliwych kluczy. Oznacza to, że ktoś przechwytujący zaszyfrowaną wiadomość mógł zamontować standardową formę ataku znaną jako kryptoanaliza brutalna. Ta metoda uruchamia możliwe klucze za pomocą algorytmu deszyfrowania do czasu znalezienia rozwiązania. Statystycznie rzecz biorąc, właściwy klucz zostaje osiągnięty po przetestowaniu tylko połowy wszystkich możliwych kluczy. Na



B6 =IF(CODE(B$2)-$A6<65,CHAR(CODE(B$2)-$A6+26+32),CHAR(CODE(B$2)-$A6+32))

CRYPTO.XLS:2

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1																					
2		E	H	Z	D	U	H	W	K	H	L	G	H	V	R	I	P	D	U	F	K
3	Key#:																				
4	1	d	g	y	c	t	g	v	j	g	k	f	g	u	q	h	o	c	t	e	j
5	2	c	f	x	b	s	f	u	i	f	j	e	f	t	p	g	n	b	s	d	i
6	3	b	e	w	a	r	e	t	h	e	i	d	e	s	o	f	m	a	r	c	h
7	4	a	d	v	z	q	d	s	g	d	h	c	d	r	n	e	l	z	q	b	g
8	5	z	c	u	y	p	c	r	f	c	g	b	c	q	m	d	k	y	p	a	f
9	6	y	b	t	x	o	b	q	e	b	f	a	b	p	l	c	j	x	o	z	e
10	7	x	a	s	w	n	a	p	d	a	e	z	a	o	k	b	i	w	n	y	d
11	8	w	z	r	v	m	z	o	c	z	d	y	z	n	j	a	h	v	m	x	c
12	9	v	y	q	u	l	y	n	b	y	c	x	y	m	i	z	g	u	l	w	b
13	10	u	x	p	t	k	x	m	a	x	b	w	x	l	h	y	f	t	k	v	a
14	11	t	w	o	s	j	w	l	z	w	a	v	w	k	g	x	e	s	j	u	z
15	12	s	v	n	r	i	v	k	y	v	z	u	v	j	f	w	d	r	i	t	y
16	13	r	u	m	q	h	u	j	x	u	y	t	u	i	e	v	c	q	h	s	x
17	14	q	t	l	p	g	t	i	w	t	x	s	t	h	d	u	b	p	g	r	w
18	15	p	s	k	o	f	s	h	v	s	w	r	s	g	c	t	a	o	f	q	v
19	16	o	r	j	n	e	r	g	u	r	v	q	r	f	b	s	z	n	e	p	u
20	17	n	q	i	m	d	q	f	t	q	u	p	q	e	a	r	y	m	d	o	t
21	18	m	p	h	l	c	p	e	s	p	t	o	p	d	z	q	x	l	c	n	s
22	19	l	o	g	k	b	o	d	r	o	s	n	o	c	y	p	w	k	b	m	r
23	20	k	n	f	j	a	n	c	q	n	r	m	n	b	x	o	v	j	a	l	q
24	21	j	m	e	i	z	m	b	p	m	q	l	m	a	w	n	u	i	z	k	p
25	22	i	l	d	h	y	l	a	o	l	p	k	l	z	v	m	t	h	y	j	o
26	23	h	k	c	g	x	k	z	n	k	o	j	k	y	u	l	s	g	x	i	n
27	24	g	j	b	f	w	j	y	m	j	n	i	j	x	t	k	r	f	w	h	m
28	25	f	i	a	e	v	i	x	l	i	m	h	i	w	s	j	q	e	v	g	l
29	26	e	h	z	d	u	h	w	k	h	l	g	h	v	r	i	p	d	u	f	k
30																					

OneTime / Vignere / KeySearch / Caesar

tabela arkusza kalkulacyjnego wyszczególnia atak brute force na szyfrogram Caesara. W tym przykładzie tekst jawny pojawia się w wierszu 6, klucz nr 3. Pamiętaj, że do ataku są wymagane trzy informacje, a wszystkie trzy są odpowiednie do szyfrowania na komputerach osobistych:

1. Znajomość zastosowanego algorytmu szyfrowania

2. Liczba możliwych kluczy

3. Język tekstu jawnego

Korzystanie z komputera w biurze nieco odbiega od wysyłania wiadomości na polu bitwy (przynajmniej w dobrym dniu). W przeciwieństwie do szpiega wroga, ktoś, kto próbuje uzyskać nieautoryzowany dostęp do danych, ma już dość dobre pojęcie o tym, który algorytm jest używany. (Jest ich stosunkowo niewiele i często są bezpośrednio związane z konkretnymi aplikacjami). Zajmuje się pierwszym elementem. Podstawową przeszkodą w ataku z użyciem siły jest drugi element, liczba kluczy. W przypadku szyfru Cezara liczba możliwych kluczy jest stosunkowo niewielka, a więc praca związana z przenoszeniem że atak może zostać zakończony bardzo szybko, co jest bardzo znaczące. Czas jest często najważniejszym czynnikiem w praktycznym kryptoanalizie. Możliwość odszyfrowania wiadomości w ciągu 24 godzin jest mało przydatna, jeśli informacje dotyczą zdarzeń mierzonych w minutach, takich jak zamówienia na zakup i sprzedaż akcji lub uruchomienie nalotów. Jeśli szyfr składa się w całości z przypadkowych substytucji listowych, takich jak to:

Plaintext: abcdefghijklmnopqrstuvwxyz

Tekst zaszyfrowany: UTWFRAQOYSEDCKJVBXGZIPHLNM

Liczba możliwych kluczy (przestrzeń kluczy) wynosi teraz 26 !, czyli ^tilde;4,03 × 10²⁶, co wygląda na jeszcze bardziej zniechęcające, gdy jest napisane:

403 291 461 126 606 000 000 000 000

Wyobraźmy sobie brutalny atak siłowy przy użyciu komputera, który może wykonać 1 milion odszyfrowania na mikrosekundę (znacznie więcej chrupania numerów niż przeciętny komputer osobisty może wykonać). Korzystanie z pojedynczego procesora może zająć ponad 10 milionów lat, aby wykonać brutalny atak na ten kod. Na szczęście dla łamacza kodu istnieją inne sposoby łamania szyfrów zastępczych, jak to omówiono za chwilę. Chodzi o to, że podczas gdy ataki brutalną siłą są możliwe, nie zawsze są one praktyczne. Chociaż prawdą jest, że przez centralne twierdzenie graniczne statystyki, najbardziej prawdopodobna liczba prób wymaganych do trafienia na prawidłowy klucz stanowi połowę całkowitej przestrzeni kluczy, średnia redukcja o współczynnik 2 jest znikoma w obliczu okresów obliczeniowych mierzony w latach i trudność w rozpoznawaniu jasnego tekstu w bagnie niewłaściwych odszyfrowań. Funkcjonalnie ataki typu brute force zależą od tego, który algorytm szyfrowania znajduje się za zaszyfrowanym tekstem. W praktyce zależą one od wykonalności sukcesów w odpowiednim czasie. Zależą one również od trzeciej informacji z powyższej listy: znajomość języka tekstu zwykłego. Rozwiązanie szyfru Caesar w Exhibit 7.5 ma tendencję do wyskakiwania, ponieważ jest bliższe zwykłemu angielskiemu niż jakiekolwiek inne rozwiązanie. Jednak bez znajomości tego, co stanowi tekst jawny, a brutalny atak siłowy będzie w najlepszym razie nieefektywny, a w najgorszym razie nieskuteczny. Ta część kryptoanalizy, rozpoznająca wynik pozytywny, jest mniej podatna na automatyzację niż jakakolwiek inna. Trudność jest potęgowana przez szyfrowanie czysto liczbowych wyników, gdzie poprawny tekst jawny może być niemożliwy do ustalenia bez rozległej dodatkowej wiedzy.

SZYFR MONOALFABETYCZNY ZASTĄPIENIOWY

Zarówno szyfr Cezara, jak i losowy szyfr zastępczy są przykładami szyfrów monoalfabetycznych. Oznacza to, że jedna litera zaszyfrowanego tekstu oznacza jedną literę tekstu zwykłego. Powoduje to, że takie kody podatne na atak różnią się od brutalnej siły. Przypuśćmy, że funkcjonariusz celny spróbuje odkryć, kiedy i jak nielegalna dostawa broni wejdzie do kraju. Następująca wiadomość jest przechwytywana:

YZYGJ KZORZ OYXZR RKZRK XUXRJ XRZXU YKQQQ

Osoba, która zakodowała ten tekst, wyraźnie zastąpiła nowe litery oryginalnych liter wiadomości. Dla doświadczonego łamacza kodów lub kryptoanalityka zadanie odszyfrowania tej wiadomości jest dość proste. Najpierw policz ile razy pojawia się każda litera w tekście. W ten sposób powstaje lista taka jak ta:

Tekst zaszyfrowany: R Z X Y K J U O G

Częstotliwość: 6 6 5 4 4 2 2 2 1

Zwróć uwagę, że ostatnie trzy litery są dyskontowane, ponieważ są po prostu wypełnianiem grupowania pięciu liter. Następnie odwołaj się do tabeli częstotliwości, która pokazuje względną częstotliwość, z jaką litery alfabetu występują w określonym języku lub dialekcie tego języka. Jedna taka lista jest pokazana poniżej

English by Letter				English by Frequency			
A	7.25	N	7.75	E	12.75	U	3.00
B	1.25	O	7.50	T	9.25	M	2.75
C	3.50	P	2.75	R	8.50	P	2.75
D	4.25	Q	0.50	I	7.75	Y	2.25
E	12.75	R	8.50	N	7.75	G	2.00
F	3.00	S	6.00	O	7.50	V	1.50
G	2.00	T	9.25	A	7.25	W	1.50
H	3.50	U	3.00	S	6.00	B	1.25
I	7.75	V	1.50	D	4.25	K	0.50
J	0.25	W	1.50	L	3.75	Q	0.50
K	0.50	X	0.50	C	3.50	X	0.50
L	3.75	Y	2.25	H	3.50	J	0.25
M	2.75	Z	0.25	F	3.00	Z	0.25

Ta lista została stworzona dla tego przykładu i proponuje, że najczęściej używanymi literami w języku angielskim w malejącej kolejności częstotliwości są e, t, r i tak dalej. Rzeczywista kolejność to prawdopodobnie e, t, a, i, o, n, s, h, r, d, l, u, kolejność kluczy na angielskiej maszynie Linotyp z XIX wieku, chociaż dokładna kolejność częstotliwości mogą się różnić w zależności od regionu pochodzenia lub przedmiotu tekstu. Zakładając, że oryginalna wiadomość jest w języku angielskim, łatwo można uzyskać listę, która dopasowuje litery kodów do liter w postaci zwykłego tekstu.

Tekst zaszyfrowany: R Z X Y K J U O G

Częstotliwość: 6 6 5 4 4 2 2 2 1

Prosty tekst: e t r i n o h s

Wynik to:

Tekst zaszyfrowany: YZYGJ KZORZ OYXZR RKZRK XUXRJ XRZXU YKQQQ

Plaintext: itiso nthet hirte enten rareo retra inqqq

Można to odczytać jako "znajduje się na trzynastce dziesięciu rzadkich pociągów rudy". Chociaż ten przykład był oczywiście wymyślony, by to podkreślić, wyraźnie ilustruje ważne narzędzie kryptograficzne, które może szybko odszyfrować coś, co na pierwszy rzut oka wydaje się bardzo nieprzyjemne. Szyfrowanie w poprzednim przykładzie mogło być oparte na prostym szyfrze zastępowania. Na przykład po użyciu hasła "TRYB", po którym następuje zwykły alfabet, bez liter w haśle dla zwykłego tekstu, zaszyfrowany tekst jest alfabetem zapisanym wstecz:

Plaintext: TRICKABDEFGHJLMNOPQSUVWXYZ

Tekst zaszyfrowany: ZYXWVUTSRQPONMLKJIHGFEDCBA

Analiza częstotliwości działa również, jeśli podstawienie jest całkowicie losowe, tak jak w przykładzie pokazanym wcześniej, którego klucz jest całkowicie losowy. Specjalistyczne narzędzia, takie jak tablice częstotliwości, które są wymagane do łamania kodów, wskazują na podstawowy kompromis: jeśli wymagany jest podstawowy poziom ochrony, łatwo jest go uzyskać, ale także łatwo go złamać, przynajmniej dla eksperta. Kwalifikacja "dla eksperta" jest ważna, ponieważ użytkownicy szyfrowania muszą zachować swoją rolę w perspektywie. Najważniejsze pytania to: Kto może zyskać dzięki odszyfrowaniu danych i jakie środki mają do dyspozycji? Nie ma sensu inwestowanie w potężny sprzęt lub oprogramowanie szyfrujące, jeśli ci próbują czytać Twoje pliki nie są szczególnie wyrafinowane,

dedykowane lub dobrze wyposażone. Na przykład osoba, która wysyła pocztówkę, wie, że może ją przeczytać każdy, kto ją zobaczy. Do tego celu można wykorzystać koperty, które nie są ostateczną poufnością, ale są szeroko stosowane i stosunkowo udane.

POLIALFABETYCZNY SZYFR ZASTĄPIENIOWY

Nawet jeśli tekst jawny używa szerszego zakresu liter niż przykład, szyfry zastępcze mogą być łamane przez analizę częstotliwości. Mocną techniką jest koncentracja na częstotliwości dwuliterowych kombinacji, znanych jako digrafy, z których najpowszechniejszym językiem w języku angielskim jest "TH". Jednym ze sposobów przeciwdziałania analizie częstotliwości jest użycie wielu zamienników dla częstszych liter. Nie można tego zrobić za pomocą prostego kodowania alfabetycznego. Jednakże, jeśli używasz liczb dla liter, możliwe jest przypisanie wielu liczby do niektórych liter, np. 13 17 19 23 dla E, które pomogłyby w rozrzedzeniu naturalnej częstotliwości tego listu. Wydaje się, że dostarczanie wielu substytucji, znanych jako homofony, proporcjonalnie do częstotliwości każdej litery, skutecznie przeciwdziała analizie częstotliwości. Jednak niektóre z podstawowych struktur tekstu jawnego wciąż istnieją, w szczególności digraphy, których kryptoanalityk może użyć do złamania kodu. W Europie w średniowieczu postępy w dziedzinie kryptografii wprowadzały państwa papieskie i włoskie miasta-państwa, aby chronić wiadomości dyplomatyczne. Następnie, w 1379 roku, Włoch Gabriele de Lavinde stworzył pierwszy europejski podręcznik kryptografia. "Ten podręcznik, teraz w archiwach Watykanu, zawiera zestaw kluczy dla 24 korespondentów i obejmuje symbole dla liter, wartości null i kilku dwuliterowych odpowiedników kodu dla słów i nazw." 15 Nazewnictwo opisane w podręczniku Lavinde " rządził całą Europą i Ameryką przez następne 450 lat" . Kilka innych godnych uwagi postępów pojawiło się w Europie w okresie podręcznika Lavinde. Po pierwsze, w 1470 roku Leon Battista Alberti opublikował pierwszy opis dysku szyfrującego. Następnie, w 1563 roku, Giambattista della Porta dostarczył pierwszy przykład digraficznego szyfrowania, w którym dwie litery są reprezentowane przez jeden symbol. Jedną z metod zmniejszania zakresu, w którym struktura tekstu jawnego odbija się w zaszyfrowanym tekście, jest szyfrowanie wielu liter. tekst jawny. Na przykład "AR" może być zaszyfrowane jako "CM". Jest to teoria kryjąca się za tak zwanym szyfrem Playfair, który został wynaleziony w 1854 roku przez brytyjskiego naukowca, Sir Charlesa Wheatstone'a, ale został nazwany na cześć jego przyjaciela Barona Playfaira którzy walczyli o jej przyjęcie przez brytyjskie Ministerstwo Spraw Zagranicznych. Chociaż szyfr Playfair pozostawał w użyciu podczas obu wojen światowych, nie robi wystarczająco dużo, aby ukryć tekst jawny i nie może wytrzymać uzgodnionej analizy częstotliwości.

SZYFR VIGENERE'A

Szczególnie ważna technika w ewolucji szyfrów polialfabetycznych ma swoje korzenie w XVI wieku. W 1586 Blaise de Vigen'ere opublikował kwadratowy stół do szyfrowania / odszyfrowywania, nazwany od niego jako Vigenere. Kwadrat i opisy pierwszych systemów autokwittyzowanego tekstu jawnego i szyfrowanego. Szyfr Vigen'a to tablica liter, taka jak ta pokazana w

	a	b	c	d	e	f	G	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	Z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	Q	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

które są używane z kluczem do zapewnienia różnych substytucji monoalfabetycznych, gdy szyfrowanie przebiega przez zwykły tekst. Zatem każda litera zaszyfrowanego tekstu ma inną relację z tekstem jawnym, tak jak poniżej:

Klucz: doomsdaydoomsdaydoomsdaydoomsday

tekst jawny: sellentireportfolionowandbuygold

szyfrogram: VSZXWQTGJIAZVGYWCMDBFPFBOJIKUKLQ

Wiadomość jest szyfrowana, patrząc na wiersz w tabeli rozpoczynający się od pierwszej litery klucza. Następnie idź wzdłuż tego rzędu, aż kolumna będzie kierowana pierwszą literą tekstu jawnego. Substytucja zaszyfrowanego tekstu jest literą na tym przecięciu w tabeli. Zatem rząd d, kolumny s, daje V. Następnie przejdź do drugiej litery i tak dalej. Uwaga że za pierwszym razem, gdy litera e jest zaszyfrowana, szyfrowana jest S, ale za drugim razem jest W. Dwa ls w sprzedaży są zakodowane odpowiednio jako Z i X, i tak dalej. Czy ten szyfr całkowicie przesłania strukturę zwykłego tekstu? Stallings zauważa: "Jeśli dwie identyczne ciągi liter w postaci zwykłego tekstu występują w odległości będącej całkowitą wielokrotnością długości słowa kluczowego, wygenerują identyczne sekwencje tekstu zaszyfrowanego." Oznacza to, że kryptoanalityk może określić długość słowa kluczowego. Po wykonaniu tej czynności szyfr można traktować jako pewną liczbę podstawień monoalfabetycznych, których liczba jest równa długości klucza. Tabele częstotliwości są ponownie uruchamiane, a kod może zostać złamany. Odpowiedź kryptografa na tę słabość polega na użyciu dłuższego klucza, który

powtarza się rzadziej. W rzeczywistości jedna technika, autokey, wymyślona przez Vigen`ere, polega na utworzeniu klucza z samego tekstu jawnego, wraz z jednym słowem kodowym, takim jak ten

Klucz: doomsdaysellentireportfolionowan

tekst jawny: sellentireportfolionowandbuygold

szyfrogram: VSZXWQTGJIAZVGYWCMDBFPFBOJILUKLQ

KRYPTOANALIZA Z POCZĄTKÓW XX WIEKU

Kryptografia rozpoczęła się wraz z wynalazkiem i rozwojem elektromagnetycznego systemu telegraficznego oraz wprowadzeniem kodu Morse'a. Samuel Morse wprowadził system kropek i kresek, które pozwalały na komunikację dalekosiężną w czasie rzeczywistym. Wyobraził sobie ten system jako środek bezpiecznej komunikacji. Inni będą musieli zaprojektować systemy do szyfrowania komunikacji telegraficznej. Anson Stager, opiekun Telegrafu Wojskowego USA podczas wojny secesyjnej, wymyślił 10 szyfrów dla armii Unii, które nigdy nie zostały złamane przez Konfederację. Użycie szyfrów telegraficznych i kodów kontynuowało się w dwóch wojnach światowych. W rzeczywistości jeden z najbardziej znanych wczesnych sukcesów kryptoanalizy spowodował wejście Stanów Zjednoczonych w I wojnę światową. Kiedy rozpoczęła się wojna, niemiecki transatlantycki kabel telegraficzny został przecięty przez Brytyjczyków, zmuszając wszystkie międzynarodowe komunikaty Niemiec do pokonania trasy. przez Wielką Brytanię przed wysłaniem na szwedzkie lub amerykańskie linie transatlantyckie.23 W 1917 r. "Brytyjscy kryptodzy odszyfrowali telegram od niemieckiego ministra spraw zagranicznych Arthura Zimmermanna do niemieckiego ministra w Meksyku, von Eckhardta. Obiecał on własności Meksyku nad terytorium należącym do Stanów Zjednoczonych (np. w Kalifornii), gdyby Meksyk przyłączył się do sprawy niemieckiej i zaatakował Stany Zjednoczone. Brytyjczycy poinformowali prezydenta Wilsona o swoim odkryciu, przekazując mu kompletny egzemplarz telegramu, w wyniku czego Stany Zjednoczone wypowiedziały wojnę Niemcom. Ten telegram stał się sławny w historii kryptoanalizy jako Telegram Zimmermanna. Druga wojna światowa odnotowała kilka zwycięstw aliantów nad potęgami Osi dzięki zastosowaniu zaawansowanych systemów kryptograficznych. Kilka z tych zwycięstw jest szerzej znanych i celebrytowanych niż pękanie niemieckiej maszyny szyfrującej Enigma, opisanej poniżej. Po odszyfrowaniu telegramu Zimmermana podczas I wojny światowej i skutkom, jakie słabe szyfry wywarły na wynik tej wojny, Niemcy szukały nierozerwalnego szyfrowania i były zainteresowane wykorzystaniem automatyzacji i wykorzystaniem maszyn do zastąpienia tradycyjnych techniki papierowe i ołówkowe. Maszyna Enigma składała się z podstawowej klawiatury, wyświetlacza, który odsłoniłby literę tekstu szyfrującego, oraz mechanizmu szyfrowania takiego, że każda litera tekstu wprowadzona jako dane wejściowe za pośrednictwem klawiatury została przepisana na odpowiadającą jej literę tekstu szyfrowania. Maszyna miała konstrukcję modułową i zastosowano wiele dysków szyfrujących w celu udaremnienia prób analizy częstotliwości. Brytyjska grupa kryptoanalizy, przy pomocy grupy polskich kryptoanalityków, po raz pierwszy złamała Enigmę już na początku II wojny światowej, a niektóre z pierwszych zastosowań komputerów były do zdekodowania szyfrów Enigmy przechwyconych od Niemców. Łamanie Enigmy było wielkim zwycięstwem aliantów, i aby nadal ją wykorzystywać, zachowywali to ukryli to w tajemnicy. Tak daleko, opisane schematy szyfrowania lub urządzenia mają zaszyfrowane wiadomości składające się ze słów i nic więcej. Jednak pojawienie się komputera, nawet w pierwotnej, podstawowej formie, zrewolucjonizowało kryptologię "w stopniu większym niż telegraf lub radio". Większość postępów kryptologów od czasu Wojny Światowej dotyczyła lub wykorzystywała komputery. W ciągu ostatnich kilku dekad algorytmy kryptograficzne przeszły do punktu, w którym ich ręczne obliczanie byłoby niewykonalne i tylko komputery mogą wykonywać wymaganą matematykę. Opieranie się na komputerach poszerzyło

informacje, które mogą korzystać z szyfrowania. Komputery używają unikalnego języka, który przekształca wszystkie informacje przechowywane na bity, każde o wartości 1 lub 0. "W rzeczywistości oznacza to że tekst jawny ma formę binarną i może być czymkolwiek; zdjęcie, głos, e-mail, a nawet wideo - nie ma znaczenia, ciąg bitów binarnych może reprezentować dowolne z nich. "

DODAWANIE XOR

W 1917 r. Inżynier z AT & T Gilbert Vernam pracował nad projektem ochrony transmisji telegraficznych przed wrogiem. W tym czasie używano teleprogramów, opartych na wersji kodu Morse'a zwanego kodem Baudota, po francuskim wynalazcy. W kodzie Baudota każda litera alfabetu ma pięć jednostek, z których każda jest albo prądem elektrycznym, albo nieobecnością prądu, znanym jako znak lub przestrzeń. Na przykład litera a jest reprezentowana przez znak, znak, spację, spację, spację. W znaczeniu binarnym każda jednostka stanowi bit, który jest albo 0 albo 1 (pięciobitowy kod dla a byłby 11000). Ten system impulsów pozwalał urządzeniom teletropowym konwertować tekst na sygnały telegraficzne i z nich za pomocą klawiatury i dziurkowanej taśmy papierowej do wprowadzania danych (otwór stanowi znak, ponieważ umożliwia urządzeniu odczytowemu nawiązanie kontaktu elektrycznego i utworzenie impulsu, podczas gdy przestrzeń jest reprezentowana pozostawiając papier nienaruszony). Każdy, kto ma odpowiednią maszynę, mógłby przechwycić i odczytać transmisję. 32 możliwe kombinacje (25) w tym kodzie zostały przypisane do 26 liter i sześciu "przecięć", które wykonały różne rzeczy, takie jak przesunięcie do wielkich liter lub przejście do następnej linii. Doskonałym pomysłem Vernama było użycie taśmy z losowymi postaciami w kodzie Baudota jako klucza, który można elektromechanicznie dodać do zwykłego tekstu. Kahn opisuje metodę dodawania w ten sposób: jeśli impulsy klawiszy i tekstu jawnego są znakami lub obydwiema spacjami, impuls zaszyfrowanego tekstu będzie spacją. Jeśli impuls klawisza jest spacją, a impuls tekstowy jest znakiem, lub odwrotnie (innymi słowy, jeśli oba są różne), zaszyfrowany tekst będzie oznaczeniem. Obecnie jest to znane jako Exclusive - lub czasami w skrócie określane jako bitowe XOR lub po prostu XOR. XOR jest szeroko stosowany w komputerowych programach szyfrujących. Zastanów się, co dzieje się podczas kodowania litery a, używając B jako klucza:

Tekst Jawny: 1 1 0 0 0 (= a)

Klucz: 1 0 0 1 1 (= B)

Tekst zaszyfrowany: 0 1 0 1 1

W pierwszej kolumnie 1 + 1 = 0, jak wskazano w Załączniku 7.8. Aby odszyfrować zaszyfrowany znak, po prostu wykonaj tę samą operację, ale dodaj zaszyfrowany tekst do klucza:

Tekst zaszyfrowany: 0 1 0 1 1

Klucz: 1 0 0 1 1 (= B)

Tekst Jawny: 1 1 0 0 0 (= a)

W momencie jego odkrycia, znaczenie tej metody tkwiło w jej zdolności do automatyzacji. Operator mógł wprowadzić tekst jawny i taśmy z kluczem do maszyny teletropowej, a następnie przesłać zaszyfrowaną wiadomość bez dalszych ludzkich danych wejściowych. Nie było wymagane przygotowanie offline. Co więcej, tak długo, jak odbiornik ma kluczową taśmę, teletropię na końcu odbiorczym automatycznie drukuje tekst jawny. To sprawiło, że system Vernama jako pierwszy zintegrował szyfrowanie z procesem komunikacji, co jest podstawową cechą systemów szyfrowania dla współczesnej komunikacji komputerowej.

DES I NOWOCZESNE SZYFROWANIE

Chociaż wykorzystywały XOR wcześniejsze komputery, fakt, że tak dobrze pracował z kodem binarnym zapewnił, że stałby się istotnym elementem nowoczesnego zestawu narzędzi kryptografa. I tak skupienie się tej części zamienia się w nowoczesną kryptografię i dwa najpowszechniej stosowane dziś kryptosystemy. Pierwszym z nich jest Data Encryption Standard (DES), a drugim jest Rivest, Shamir, Adleman (RSA).

RZECZYWISTE OGRANICZENIA

Jak sugeruje poprzedni przegląd ewolucji szyfrowania, znaczące postępy, które są bardzo nieliczne, często wiążą się z osobami, które je stworzyły, takimi jak Vigen`ere, Playfair i Vernam, z których żaden nie miał korzyści z komputerów. Dzisiejsze skomputeryzowane systemy szyfrowania zazwyczaj wykorzystują szereg klasycznych technik, które po połączeniu eliminują lub minimalizują niedociągnięcia jakiejkolwiek pojedynczej metody. Omówimy tu kilka technik, w tym transpozycję i wirniki, które wskazują drogę do najczęściej stosowanego schematu szyfrowania do tej pory: DES. Najpierw jednak weź pod uwagę praktyczne problemy napotkane przez Vernama, który w inny sposób był genialny. Vernam zaproponował klucz, który był długim ciągiem losowych znaków. Zostało to zakodowane na pętli taśmy papierowej, która ostatecznie się powtórzyła (taśma zawierała około 125 znaków na stopę). Długość klucza spowodowała, że kryptoanaliza przechwyconych wiadomości była niezwykle trudna, ale nie niemożliwa, ponieważ ostatecznie klucz został powtórzony. Przy wystarczającej ilości zaszyfrowanego tekstu kod poddałby się analizie częstotliwości. (Pamiętaj, że w czasie wojny, a nawet ćwiczeń wojskowych, setki tysięcy słów może być zaszyfrowanych dziennie, zapewniając solidną podstawę do kryptoanalizy).

SZYFR Z KLUCZEM JEDNORAZOWYM

Zaproponowano kilka ulepszeń, aby uniknąć niepraktyczności tworzenia po prostu dłuższych i dłuższych taśm z kluczami. Inny inżynier AT & T, Lyman Morehouse, zaproponował użycie dwóch kluczowych taśm o długości około ośmiu stóp, zawierających około 1000 znaków, w celu wygenerowania ponad 999 000 kombinacji znaków. który może zostać wprowadzony do procesu szyfrowania jako klucz. Była to poprawa pod względem praktyczności i bezpieczeństwa, ale, jak zauważył major Joseph Mauborgne z Korpusu Sygnałów Armii USA, ciężki ruch wiadomości zaszyfrowany w ten sposób nadal może zostać zdekodowany. To Mauborgne zdał sobie sprawę, że użyje jedynego niezłomnego szyfru klucze, które Kahn określa jako "nieskończone i bezsensowne". Tak więc wymyślił coś, co znamy jako system jednorazowy, jedyny niezniszczalny schemat szyfrowania. Jednorazowy system jest czasem nazywany jednorazowym padem, ponieważ jest to sposób, w jaki został on wdrożony przez agentów wywiadu w terenie. Agent jest wystawiony pad, który wyrównuje kolumny i wiersze całkowicie losowych znaków. Pierwsza litera tekstu jawnego jest szyfrowana przy użyciu odpowiedniego zaszyfrowanego tekstu z wiersza 1, druga litera jest szyfrowana z wiersza 2 i tak dalej. Wynikiem jest tekst zaszyfrowany, który nie zawiera statystycznej zależności od zwykłego tekstu. Po zaszyfrowaniu wiadomości pad zostaje zniszczony. Odbiorca, który ma kopię pada, używa jej do odwrócenia procesu i odszyfrowania wiadomości. Jednorazowy pad zasadniczo jest polialfabetycznym szyfrem zastępczym, ale z tą samą liczbą alfabetów, co znaki w komunikacie, w ten sposób pokonując wszelkie rodzaj analizy częstotliwości. Atak brute force zostaje pokonany przez fakt, że każdy możliwy wynik jest statystycznie istotny jak każdy inny. Jak wskazuje Kahn, czterocyfrowa grupa zaszyfrowanego tekstu mogłaby równie dobrze dać pocałunek, szybkość, powolność lub jakąkolwiek inną możliwą czteroliterową kombinację. Dlaczego więc nierozerwalny jednorazowy system nie jest uniwersalny? Cóż, pozostaje ulubieńcem agentów wywiadowczych w terenie, którzy od czasu do czasu potrzebują wysyłać krótkie wiadomości. Jednak w przypadku szyfrowania komercyjnego lub militarnego na dużą skalę, nie udało się rozwiązać problemu wielkości klucza, który system Vernama ujawnił. Klucz musi być tak duży, jak całkowita objętość zaszyfrowanych informacji, i istnieje stałe

zapotrzebowanie na nowe klucze. Co więcej, zarówno nadawca, jak i odbiorca muszą trzymać i bronić identycznych kopii tego ogromnego klucza.

TRANSPOZYCJA, WIRNIKI , PRODUKTY I BLOKI

Zupełnie inną techniką od substytucji jest transpozycja. Zamiast zastępowania znaków zaszyfrowanych tekstem jawnym, szyfr transpozycji zmienia kolejność znaków w postaci zwykłego tekstu. Najprostszy przykład jest nazywany ogrodzeniem kolejowym. Na przykład, aby zaszyfrować "sprzedaj całe portfolio teraz i kupuj złoto", każda postać jest zapisywana na alternatywnych liniach, tak jak poniżej:

sletrprflooadugl

elnieotoinwnbyod

co skutkuje tym zaszyfrowanym tekstem:

SLETRPRFLFLADADLELNIEOTOINWNBYOD

Jak dotąd nie stanowi to poważnego wyzwania. Bardziej wymagająca jest następna transpozycja do wierszy i kolumn ponumerowanych klawiszem (w tym przypadku 37581426), tak aby pierwszy zestaw znaków tekstu zaszyfrowanego miał mniej niż 1, drugi mniejszy niż 2 itd.

Tekst zaszyfrowany: EROGTFALSRLDNTWOLPOUIONDEEIBLONY

Chociaż jest to bardziej złożone, transpozycja ta nadal ulegnie kryptoanalizie, ponieważ zachowuje charakterystykę częstotliwości liter tekstu jawnego. Analityk będzie również poszukiwał dwuznaków i trigrafii podczas zabawy z kolumnami i rzędami różnej długości. (Kahn opisuje francuskie łamacze kodów podczas I wojny światowej dosłownie przecinając tekst na paski i przesuwanie ich w górę i w dół względem siebie, aby przełamać niemieckie szyfry transpozycji). To, co sprawia, że transpozycja jest trudna do odczytania, jest dodatkowym etapem szyfrowania. Na przykład, jeśli poprzedni tekst zaszyfrowany jest ponownie uruchamiany przez system, używając tego samego klucza, wydaje się, że pozór wzorca zniknął.

Tekst zaszyfrowany: TNILAWNESLEFTOOOLOILODYRRPEGDUB

Rozwój coraz bardziej złożonych szyfrów wielowprowadzeniowych wskazywał na pozytywne efekty wielu etapów szyfrowania, które mają również zastosowanie do szyfrów zastępczych. Najlepszymi tego przykładami są maszyny wirnikowe używane przez Niemców i Japończycy podczas II wojny światowej. Niektóre spostrzeżenia zdobyte podczas ataku na niemieckie kodeksy, takie jak praca Alana Turinga z 1940 r. Dotycząca zastosowania statystyk informacyjnych do kryptoanalizy, uznano za tak ważne, że pozostawały one klasyfikowane przez ponad 50 lat. Chociaż ostatecznie zostali pokonani przez alianckie kryptoanalityki, systemy elektromechaniczne, takie jak Enigma, były nie tylko najbardziej wyrafinowanymi systemami szyfrowania przedsystemowego, ale również ich złamanie było głównym katalizatorem rozwoju samych systemów komputerowych. Kiedy ludzie zaczęli stosować systemy komputerowe do tworzenia kodu, a nie do łamania kodu, szybko wpadli na pomysł rozcinania zwykłego tekstu na kawałki lub bloki, aby ułatwić obsługę.

Termin "szyfr blokowy" jest używany do opisywania szyfrów, które szyfrują jeden blok (na przykład 8 bajtów danych) na raz, jeden blok po drugim. Kolejnym rezultatem skomputeryzowania procesu szyfrowania jest klasa szyfrów znana jako szyfry produktu. Szyfr produktu został zdefiniowany jako "szyfr blokowy, który iteruje kilka słabych operacji, takich jak podstawianie, transpozycja, modułowe dodawanie / mnożenie [takie jak XOR] i transformacja liniowa." Matematyka szyfrów produktu wykracza poza zakres tej części, ale warto zauważyć, że "[n] obody wie, jak udowodnić matematycznie,

że szyfr produktu jest całkowicie bezpieczny. . . Szyfr produktu powinien działać jako funkcja "mieszania", która łączy w sobie tekst jawny, klucz i tekst zaszyfrowany w złożony, nieliniowy sposób. "Części szyfru produktu, które wykonują rundy podstawienia, są nazywane S-boxami. Szyfr produktu o nazwie Lucyfer ma dwa z tych S-boxów, podczas gdy DES Szyfrowanie ma osiem S-boxów. Zdolność szyfru produktu do generowania prawdziwie losowego nieliniowego tekstu zaszyfrowanego zależy od starannego zaprojektowania tych S-boxów. Przykłady współczesnych szyfrów produktów obejmują Lucyfer (opracowany przez IBM), DES (opracowany przez IBM / NSA), LOKI (Brown, Pieprzyk i Seberry) oraz FEAL (Shimizu i Miyaguchi). Klasa szyfrów Feistel działa na połowie zaszyfrowanego tekstu w każdej rundzie, a następnie zamienia połówki tekstu zaszyfrowanego po każdej rundzie. Przykładami szyfrów Feistela są Lucyfer i DES, oba są systemami komercyjnymi

STANDARD SZYFROWANIA DANYCH

Tradycyjnie główne rynki dla twórców kodu i twórców komputerów są takie same: rządy i banki. Po II wojnie światowej komputery zostały opracowane do celów wojskowych i komercyjnych. W połowie lat 60. wiodącym producentem komputerów był IBM, który mógł dostrzec, że rosnąca rola komunikacji elektronicznej w handlu stworzy ogromny rynek dla niezawodnych metod szyfrowania. Przez wiele lat matematycy i informatycy, w tym Horst Feistel w laboratorium badawczym IBM w Yorktown Heights, Nowy Jork, opracował szyfr Lucyfer, który został sprzedany Lloyds of London w 1971 roku do użytku w systemie wydawania pieniędzy. Amerykańska Agencja Bezpieczeństwa Narodowego (NSA) była w ścisłym kontakcie z projektem Lucifera, regularnie odwiedzając laboratorium (stała przepływ personelu między NSA, IBM i działami matematyki głównych uniwersytetów amerykańskich dążył do ścisłego monitorowania wszystkich nowych wydarzeń w tej dziedzinie). W przybliżeniu w tym samym czasie Krajowe Biuro Standardów (NBS) opracowywało standardowe specyfikacje bezpieczeństwa dla komputerów używanych przez rząd federalny. W 1973 roku NBS zaprosił firmy do zgłaszania kandydatów na algorytm szyfrowania, który ma zostać przyjęty przez rząd w celu przechowywania i przesyłania niesklasyfikowanych informacji. (Rząd przetwarza wiele informacji, które są wrażliwe, ale niewystarczająco istotne dla bezpieczeństwa narodowego, aby uzasadnić klasyfikację.) IBM przedłożył NBS zmienną swojego szyfru Lucifera, a po szerokich testach przeprowadzonych przez NSA, ten szyfr został przyjęty jako Standard szyfrowania danych (DES). Akronim w rzeczywistości odnosi się do dokumentu opublikowanego w publikacji Federalnej Normy przetwarzania informacji 46 lub FIPS PUB 46 w skrócie. Zostało to opublikowane 15 stycznia 1977 roku, a DES stał się obowiązkowy dla wszystkich "departamentów federalnych i agencji, dla każdego…dane niezwiązane z bezpieczeństwem międzynarodowym. "37 Mandat federalny stwierdził również, że należy zachęcać organizacje komercyjne i prywatne do korzystania z DES.38 W rezultacie DES stał się szeroko stosowany, szczególnie w branży bankowej.39 Sercem DES jest szyfrowanie danych Algorytm (DEA), opisany w publikacji American National Standards Institute, zatytułowany American National Standard for Information Systems-Data Encryption Algorithm-Modes of Operation, 1983, jako ANSI X3.106-1983.

WYTRZYMAŁOŚĆ DES

DES stał się i pozostał faktycznym standardem komercyjnego kodowania do późnych lat dziewięćdziesiątych, kiedy wątpliwości co do jego siły w stosunku do szybkiego postępu w sprzęcie komputerowym i oprogramowaniu doprowadziły do poszukiwania ewentualnej wymiany. Jednak DES jest nadal szeroko stosowany, więc przed omówieniem jego wymiany konieczne jest bardziej szczegółowe omówienie jego użycia. Pierwszą rzeczą, na którą należy zwrócić uwagę, jest to, że jedyną znaną metodą rozszyfrowania danych zaszyfrowanych za pomocą DES bez znajomości klucza jest użycie brutalnej siły. Obejmuje to skomputeryzowane porównanie danych w postaci zwykłego tekstu z zaszyfrowanymi wersjami tych samych danych, przy użyciu każdego możliwego klucza do obu wersji

dopasowanie danych. W przypadku DES liczba możliwych kombinacji wynosi około 70 biliardów. To bardzo duża liczba, a wypróbowanie wszystkich kombinacji w ciągu mniej niż kilku lat wymaga stosunkowo drogiego sprzętu (lub starannie zaaranżowanej aplikacji dużych ilości taniego sprzętu). Technicznie rzecz biorąc, DEA jest połączonym szyfrem podstawienia / transpozycji, szyfru produktu, który działa na blokach danych o długości 64 bitów lub 8 bajtów. Korzystanie z 56 bitów dla klucza wytwarzają przestrzeń kluczy 256 lub 2 057 994 037 927 940, liczbę w regionie wynoszącą 70 biliardów. Trudność ataku na DES może zostać zwiększona dość łatwo, jeśli zastosuje się podwójne lub potrójne szyfrowanie, ale mimo to zawsze było coś z chmury nad DES. W momencie zatwierdzenia DEA, dwóch profesorów Uniwersytetu Stanforda, którzy są wybitnymi w kryptografii XX wieku, Martin Diffie i Whitfield Hellman, wskazało, że algorytm, zatwierdzony przez NBS, będzie coraz bardziej narażony na atak, ponieważ sprzęt komputerowy zwiększył moc i obniżył koszty.

SŁABOŚĆ DES

Jak pisze autor George Sassoon: "Chociaż zarówno Departament Handlu Stanów Zjednoczonych, jak i Zjednoczone Królestwo, energicznie to robią, wszyscy wiedzą, że NSA wymusiła zmniejszenie długości klucza DES o połowę, aby sami mogli złamać szyfry, nawet jeśli nikt inny nie byłby w stanie tego zrobić." Chociaż NBS odrzucił taką krytykę, a NSA kategorycznie zaprzeczyła, że stoją za wszelkimi próbami osłabienia szyfru, opinia ta uzyskała pewne wsparcie ze strony NSA w 1986 r., Kiedy agencja ogłosiła, że nie będzie już poświadczać DEA z tytułu niesklasyfikowanego użycia, mniej niż 10 lat po zatwierdzeniu DES. Ten ruch był spowodowany szybkim rozwojem Komputery równoległe, które osiągają niesamowite możliwości przetwarzania, wykorzystując setki lub nawet tysiące procesorów pracujących równolegle. Maszyny te oferują ogromną moc przy znacznie niższych kosztach niż tradycyjne superkomputery. Być może NSA dostrzegł nieuchronność czegoś takiego jak EFF DES Cracker, który został zbudowany w 1998 roku za mniej niż 250 000 $ i złamał szyfrowaną wiadomość DES w mniej niż trzy dni. Oryginalny szyfr Lucyfera używał bloków danych 128-bitowych i klucza 112-bitowego. Gdyby to było przestrzegane w DEA, różnica w liczbie możliwych kombinacji klawiszy byłaby oszałamiająca. Chociaż 2⁵⁶, bieżący keyspace, jest liczbą większą niż 7 z 16 zerami za nim, 2¹¹² jest większe niż 5, z 33 zerami za nim. Praktyczna konsekwencja tej słabości w DEA pozostała po stronie popytu na silniejsze algorytmy i pojawiły się obiecujące nowe, takie jak Blowfish Bruce'a Schneiera. Nadal istnieją pewne pozytywne aspekty DES, które sprawiają, że jest on opłacalny dla niektórych zastosowań komercyjnych. Jak wspomniano wcześniej, słabość kryptograficzna DES może być łatwo wzmocniona podwójnym szyfrowaniem, co podwaja trudność odszyfrowania, wnosząc to zadanie w sferę superkomputerów i specjalnie zbudowanych, masowo równoległych maszyn. Fakt, że DES jest standardem od tak dawna, oznacza, że DES jest teraz dostępny w wielu formach, takich jak implementacje jednoukładowe, które można wstawić do gniazd ROM i zintegrować z wszelkimi urządzeniami, takimi jak karty rozszerzeń, karty PCMCIA, i karty inteligentne.

SZYFROWANIE KLUCZEM PUBLICZNYM

Nawet z dłuższym kluczem, DEA nadal będzie miał poważną słabość, którą dzieli z wszystkimi innymi wspomnianymi do tej pory systemami szyfrowania klucza prywatnego. Ta słabość oznacza potrzebę zachowania klucza w tajemnicy.

PROBLEM WYMIANĄ KLUCZA

Kiedy dane chronione hasłem są przesyłane z jednego miejsca do drugiego, elektronicznie lub ręcznie, potrzeba przekazania hasła odbiorcy stanowi poważne przeszkody. W kryptografii są one znane wspólnie jako problem wymiany klucza. Tak opisuje ją Crypt Cabal40: Jeśli chcesz, aby Twoi znajomi mogli wysyłać tajne wiadomości do Ciebie, musisz upewnić się, że nikt inny niż oni nie widzi klucza…. [Jest to] jeden z najbardziej dokuczliwych problemów całej wcześniejszej kryptografii: konieczność

ustanowienia bezpiecznego kanału do wymiany klucza. Aby ustanowić bezpieczny kanał, używa się kryptografii, ale kryptografia klucza prywatnego wymaga bezpiecznego kanału! Tak więc nawet przy użyciu bardzo wydajnych systemów klucza prywatnego, takich jak DES, hasło lub dystrybucja kluczy jest poważnym problemem. Po tym wszystkim, powód do szyfrowania cennych informacji w pierwszej kolejności dlatego, że zakłada się ktoś próbuje ukraść lub manipulować nim. Oznacza to zmotywowanego i wyszkolonego przeciwnika. Taki przeciwnik prawdopodobnie wykorzysta każdą okazję, aby odkryć hasło, które odblokuje informacje. Hasło jest prawdopodobnie najbardziej zagrożone przez takiego przeciwnika, gdy jest przekazywane z jednej osoby na drugą. Chociaż brzmi to jak film Bonda, jest to bardzo realny i praktyczny problem, z którym trzeba się było zmierzyć w wielu obszarach legalnej, zorganizowanej działalności, od firm po instytucje publiczne, nawet wtedy, gdy dostępny jest skomputeryzowany system szyfrowania oparty na DEA. Załóżmy, że zaszyfrowany plik wrażliwych danych księgowych musi dotrzeć do siedziby głównej. W jaki sposób odbiorca zna hasło potrzebne do uzyskania dostępu do pliku? Nadawca mógł wykonać połączenie telefoniczne. Ale czy będzie to podsłuchane? W jaki sposób należy zweryfikować tożsamość osoby na drugim końcu? Kuriera można było wysłać z zapieczętowaną kopertą. Hasło może być zaszyfrowane. Ale wszystkie te kanały stanowią problem. Jak zagwarantować, że kurier jest uczciwy lub czy koperta dotrze nienaruszona? A jeśli hasło zostanie zaszyfrowane, będzie potrzebowało hasła, które będzie musiało zostać przesłane. Odbiorca pliku może otrzymać hasło przed wiadomość jest szyfrowana, ale nie ma gwarancji, że hasło nie zostanie przechwycone. Istnieją sposoby na utrudnianie atakującym spraw, ale idealnym rozwiązaniem byłoby użycie klucza, który był bezużyteczny dla atakującego.

SYSTEMY KLUCZA PUBLICZNEGO

System szyfrowania klucza publicznego oferuje szyfrowanie, które nie zależy od klucza odszyfrowywania, który pozostaje tajemnicą. Pozwala również odbiorcy kluczy i komunikatów na sprawdzenie źródła. Pierwszy opublikowany opis kryptosystemu klucza publicznego pojawił się w 1976 roku, autor: profesor Uniwersytetu Stanford Martin Hellman i badacz Whitfield Diffie. Ralph Merkle niezależnie przybył do podobnego systemu. Ralph Merkle po raz pierwszy zaproponował ideę kryptografii klucza publicznego w 1974 r., A Martin Hellman i Whitfield Diffie przedstawili tę samą ideę na forum publicznym w 1976 r. Pomysł ten uznano za przełomowy przełom, "ponieważ nie przyszło to nikomu innemu w długiej historii kryptologii, że kluczem odszyfrowującym może być coś innego niż odwrotność klucza szyfrującego." System Diffiego-Hellmana stosuje formę matematyki zwaną arytmetyką modułową. "Modułowa arytmetyka jest sposobem ograniczania wyniku podstawowych operacji matematycznych do zbioru liczb całkowitych z wyższym ograniczeniem." Doskonały przykład tej matematycznej zasady można znaleźć poprzez zbadanie zegara militarnego: Rozważmy zegar czasu militarnego, według którego godziny są mierzone tylko w zakresie od zera do 23, przy czym zero odpowiada północy i 23 do 11 godzinie w nocy. W tym systemie postęp z 25 godzin na godzinie trzeciej nie prowadzi nas do godziny 28, ale pełne koło do godziny 4 (ponieważ 25 + 3 = 28 i 28 - 24 = 4). W tym przypadku liczba 24, górna granica operacji obejmujących pomiar godzin, jest nazywana modułem. Kiedy obliczenia obejmujące godziny na zegarze dają dużą liczbę, odejmujemy liczbę 24, aż otrzymamy liczbę całkowitą od 0 do 23, proces znany jako redukcja modułowa. Pomysł ten można rozszerzyć na moduły o różnych rozmiarach Protokół Diffiego-Hellmana pozwala dwóm użytkownikom wymieniać klucz symetryczny na niezabezpieczony nośnik bez wcześniejszych wspólnych tajemnic. Protokół zawiera dwa publicznie znane i szeroko rozpowszechnione parametry systemowe: p, dużą liczbę całkowitą całkowitą, która wynosi 1024 bity, 45 i g, liczbę całkowitą mniejszą niż p. Dwaj użytkownicy, którzy chcą się komunikować, są nazywani Alice i Bobem ze względu na prostotę. Postępują w ten sposób. Po pierwsze, Alicja generuje losową wartość prywatną a, a Bob generuje losową wartość prywatną b. Zarówno a, jak i b są [mniej niż p]. Następnie wyprowadzają swoje wartości publiczne za pomocą parametrów p i g oraz ich wartości prywatnych. Publiczna wartość Alice to g^a mod p, a

publiczna wartość Boba to g^b mod p. Następnie wymieniają swoje wartości publiczne. Na koniec Alice oblicza $g^{ab} = (g^b)^a$ mod p, a Bob oblicza $g^{ba} = (g^a)^b$ mod p. Ponieważ $g^{ab} = g^{ba} = k$, Alice i Bob mają teraz wspólny klucz tajny k. Protokół ten wprowadził pojęcie do kryptografii znane jako dyskretny problem z logami. "Dyskretny problem z logami jest następujący: podane g, p, i g^x mod p, co to jest x? " Ogólnie rzecz biorąc, we wszystkich społecznościach matematycznych i kryptologicznych powszechnie przyjmuje się, że dyskretny problem z logiem jest trudny do rozwiązania, na tyle trudny, aby algorytmy mogły na nim polegać ze względów bezpieczeństwa. Algorytm przeprowadzania szyfrowania kluczem publicznym opublikował w 1977 r. Ronald Rivest z MIT, Adi Shamir z Instytutu im. Weizmanna w Izraelu i Leonard Adleman z University of Southern California. Tych trzech mężczyzn stworzyło RSA Data Security Company, która otrzymała wyłączną licencję na patent, który MIT uzyskał na ich algorytmie. Duża liczba licencjonowanych programów dla firm opartych na tym algorytmie, od AT & T do IBM i Microsoft. Algorytm RSA działa obecnie we wszystkim, od zakupów online po telefony komórkowe. Ponieważ rozwiązanie tajnego dylematu klucza, kryptografia klucza publicznego została przez wielu uznana za rewolucyjną technologię ", co stanowi przełom, który sprawia, że rutynowe szyfrowanie komunikacji staje się praktyczne i potencjalnie wszechobecny ", zgodnie z FAQ Sci.Crypt, który stwierdza: W kryptosystemie klucza publicznego, EK może być łatwo wyliczony z jakiegoś klucza publicznego X, który z kolei jest liczony od K. X, więc każdy może szyfrować wiadomości. Jeśli odszyfrowanie DK nie może być łatwo wyliczone z klucza publicznego X bez znajomości klucza prywatnego K, ale łatwo ze znajomością K, to tylko osoba, która wygenerowała K może odszyfrować wiadomości. Matematyczne zasady, które to umożliwiają, wykraczają poza zakres tej części. Więcej szczegółów można znaleźć w "Często zadawanych pytaniach na temat dzisiejszej kryptografii" RSA Laboratories, który jest dystrybuowany przez RSA Data Security, firmę, która sprzedaje produkty w oparciu o Algorytm RSA. W skrócie, szyfrowanie klucza publicznego jest możliwe, ponieważ niektóre obliczenia są trudne do odwrócenia, co zostało wskazane przez Diffiego i Hellmana, którzy po raz pierwszy opublikowali pomysł szyfrowania klucza publicznego. Oto w jaki sposób RSA opisuje obliczenia, które umożliwiają (z niewielkimi wyjaśnieniami od autora):

Załóżmy, że Alicja chce wysłać prywatną wiadomość, m, do Boba. Alice tworzy zaszyfrowany tekst c, potęgując:

$c = m^e$ mod n

gdzie e oraz n są kluczem publicznym Boba. Aby odszyfrować, Bob również potęguje:

$m = c^d$ mod n

gdzie d jest prywatnym kluczem Boba. Bob odzyskuje oryginalną wiadomość, m; relacja między e a d zapewnia, że Bob poprawnie odzyskuje m. Ponieważ tylko Bob zna d, tylko Bob może odszyfrować. Jest to przedstawione na rysunku, który jest zgodny z opisanym scenariuszem. Dolna część diagramu używa liczb wziętych z przykładu podanego przez Stallings. Liczby te są znacznie mniejsze niż rzeczywiste liczby używane przez RSA. Chodzi o to, że biorąc pod uwagę tekst zaszyfrowany (c) i klucz publiczny (e, n) oraz znajomość algorytmu, odczytywanie komunikatu (m) jest wciąż niepraktyczne. Dzieje się tak dlatego, że n tworzy się przez pomnożenie dwóch liczb pierwszych (zwykle reprezentowanych jako p i q), a e otrzymuje się z n połączonego z kluczem tajnym, d. Aby złamać szyfr, musisz złożyć dużą liczbę na parę liczb pierwszych. Jak duży? Ma ponad 150 cyfr (czyli cyfry, a nie bity). Ta kryptoanaliza jest bardzo trudna do wykonania w znaczącym okresie czasu, nawet w przypadku bardzo wydajnego komputera. Duże sieci komputerów zostały z powodzeniem uwzględnione

1. Wybrany klucz prywatny

Wybierz dwie liczby pierwsze, p i q p = 7 i q = 17

2. Klucz publiczny, obliczony

Oblicz n = pq 7 × 17 = 119

3. Wybrany klucz publiczny

Oblicz ϕ (n) = (p - 1) (q - 1) = 96

Wybierz e, tak, aby e było względnie pierwsze w ϕ(n) i < ϕ (n) e = 5

4. Klucz prywatny, obliczony

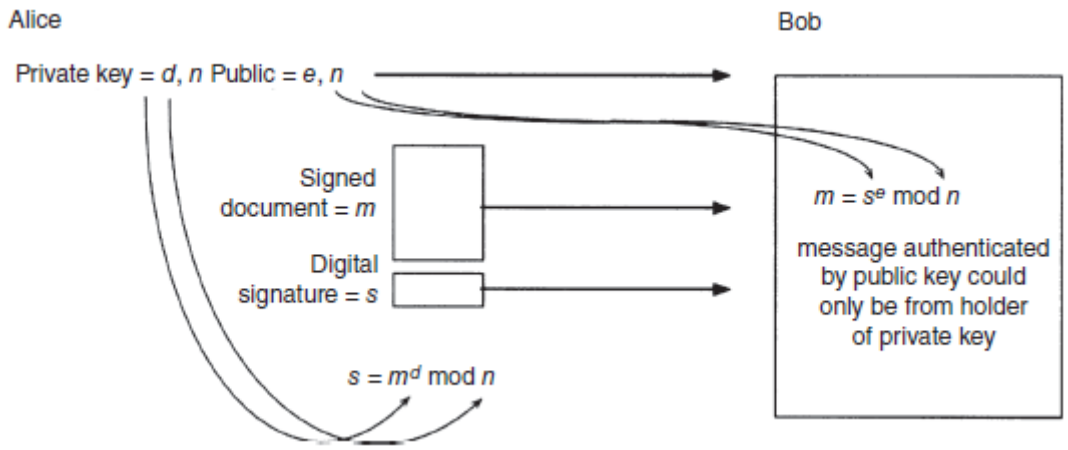
Wyznaczyć d, tak, aby de = 1 mod 96 i d <96 Ponieważ 77 x 5 = 385 = 4 x 96 + 1 d = 77

Wynik; Klucz publiczny, KU = 5,119 Klucz prywatny, KR = 77 119

100-cyfrowa liczba na dwie liczby pierwsze, ale algorytm RSA może używać liczb nawet większych, jeśli algorytmy zasilania i faktorowania zaczynają nadążać za bieżącymi implementacjami.

AUTENTYCZNOŚĆ I ZAUFANIE

Punkt kryptosystemów klucza publicznego nie jest zagrożony przez dystrybucję haseł. Ponieważ klucze są uważane powszechnie znane, niektóre elementy "muszą być opracowane do świadczyć o autentyczności, ponieważ posiadanie samych kluczy (wystarczająca do zaszyfrowania wiadomości zrozumiałe) ma dowodów konkretnej unikalnej tożsamości nadawcy", zgodnie z sci.crypt FAQ , Klucze są faktycznie tymi z danych bytów. Mechanizmy wyszukiwania polegają na zaufanych uprawnieniach, które mogą nie generować kluczy. Inne podejście zostało nazwane Pretty Good Privacy lub PGP. Jest to podejście "Web of trust", które polega na tym, że użytkownicy rozpowszechniają i śledzą nawzajem swoje klucze i ufają nieformalnemu, rozproszonemu sposobowi. Oto w jaki sposób RSA może być użyty do wysłania dowodu tożsamości nadawcy oprócz zaszyfrowanej wiadomości. Po pierwsze, niektóre informacje są szyfrowane kluczem prywatnym nadawcy. To jest podpis i jest zawarty w wiadomości. Odbiornik może "użyć algorytmu RSA w odwrotnej kolejności do weryfikacji informacji nie odszyfrowuje rozsądnie, szukając nie tylko dana jednostka Mogło zaszyfrowany tekst jawny przez wykorzystanie tajnego klucza." Co oznacza "odszyfrowuje rozsądnie" oznacza? Odpowiedź obejmuje coś, co nazywa się podsumowaniem wiadomości, które jest "unikalnym matematycznym podsumowaniem tajnej wiadomości". Teoretycznie tylko nadawca wiadomości może wygenerować swój ważny podpis dla tej wiadomości, tym samym uwierzytelniając ją dla odbiorcy. Oto jak opisuje RSA uwierzytelnianie, zgodnie z diagramem



Załóżmy, że Alicja chce wysłać podpisany dokument do Boba. Alice tworzy cyfrową sygnaturę s,

potęgując: $s = m^d \bmod n$, gdzie d i n należą do pary kluczy Alice. Wysyła i m do Boba. Aby zweryfikować podpis, Bob potęguje i sprawdza, czy wiadomość została odzyskana: $m = s^e \bmod n$, gdzie e i n należą do klucza publicznego Alicji.

OGRANICZENIA I KOMPBINACJE

Jak wspomniano wcześniej, wiele produktów używa dziś RSA, w tym Microsoft Windows, Lotus Notes, Adobe Acrobat, Netscape Navigator, Internet Explorer i wiele innych. W większości z tych przykładów RSA jest wykorzystywany raczej do uwierzytelniania niż do szyfrowania danych na dużą skalę. To dlatego, że są one bardzo zauważalne: są powolne. Jest to równoważone faktem, że są trudniejsze do zerwania. Według RSA, DES jest generalnie co najmniej 100 razy szybszy niż RSA po zaimplementowaniu w oprogramowaniu. W sprzęcie DES jest od 1000 do 10 000 razy szybszy, w zależności od implementacji. RSA może zmniejszyć lukę w nadchodzących latach w miarę rozwoju bardziej specjalistycznych układów. Jednak algorytmy klucza publicznego raczej nie dorównają wydajności szyfrów kluczy prywatnych, takich jak DES. Na szczęście istnieje proste rozwiązanie: "Użyj algorytmu klucza prywatnego do szyfrowania danych, ale użyj systemu klucza publicznego do obsługi wymiany kluczy i uwierzytelniania. RSA Data Security lub Blowfish firmy Schneier, który jest dostępny bezpłatnie. DES, oprócz RSA są inne systemy publiczne. Jedna metoda, zwana SEEK, jest opatentowana, opatrzona znakiem towarowym i sprzedawana przez firmę Cylink z Sunnyvale w Kalifornii. Ta metoda używa alternatywnego algorytmu do dystrybucji klucza publicznego. Cylink produkuje szereg szyfratorów DES, które używają SEEK do dystrybucji kluczy.

SZYFROWANIE PRAKTYCZNE

Podstawowym rynkiem systemów i urządzeń szyfrujących jest komunikacja. Jednak rozwój handlu internetowego zaowocował szeregiem nowych i interesujących składników kryptograficznych, które mają znaczną wartość dla bezpieczeństwa komputerowego.

KOMUNIKACJA I PRZECHOWYWANIE

Jeśli spojrzysz na komercyjne produkty z listy NIST (National Institute of Standards and Technology), które są zatwierdzone, większość z nich jest zaprojektowana tak, aby chronić informacje, gdy są przekazywane, a nie kiedy siedzi na komputerze do lokalnego użytku. Jest to zrozumiałe, gdy spojrzysz na rozwój komputerów, który rozprzestrzenił się na zewnątrz od "mainframe fortecznego". Scentralizowane magazyny danych nadają się do fizycznej kontroli dostępu. Szyfrowanie danych pozostających w tyle za ścianami i zamkniętymi drzwiami może być przesadzone w tym scenariuszu, szczególnie gdy ma miejsce kara za wydajność. Szyfrowanie było zarezerwowane dla danych przesyłanych między komputerami przez przewody. Ta filozofia została rozszerzona na serwery plików w sieciach. Szyfrowanie plików na serwerze nie było uważane za priorytet, ponieważ ludzie zakładali, że serwer będzie chroniony. Szyfrowanie danych na samodzielnych urządzeniach i nośnikach wymiennych jest stosunkowo nowym rozwiązaniem, zwłaszcza że coraz więcej poufnych danych jest umieszczanych w fizycznie mniejszych i mniejszych urządzeniach. Obecnie istnieje wiele produktów, za pomocą których można zaimplementować szyfrowanie plików.

ZABEZPIECZENIE WARSTWY TRANSPORTOWEJ

Jednym z najbardziej widocznych przykładów szyfrowania w pracy w dzisiejszym zabezpieczeniach komputerowych jest ikona bezpieczeństwa, którą widzą ludzie w przeglądarce internetowej; Jest to przykład czegoś, co nazywa się zabezpieczeniem warstwy transportowej, które używa protokołów o nazwach SSL i TLS.

POPULARNE PROTOKOŁY

SSL oznacza Secure Sockets Layer, protokół szyfrowania oprogramowania opracowany przez Netscape i pierwotnie zaimplementowany w Netscape Secure Server i przeglądarce Netscape Navigator. Protokół SSL jest również obsługiwany przez program Microsoft Internet Explorer i wiele innych produktów. TLS oznacza Transport Layer Security, nazwę nadaną standardowi internetowemu opartemu na SSL, przez IETF (jak w Internet Engineering Task Force, RFC 2246). Istnieją niewielkie różnice między protokołami SSLv3.0 i TLSv1.0, ale nie ma znaczących różnic pod względem siły zabezpieczeń, a oba protokoły współpracują ze sobą. TLS jest protokołem, standardową procedurą do regulowania transmisji danych między komputerami. W rzeczywistości składa się z dwóch warstw protokołu. Na najniższym poziomie znajduje się Protokół Zapisu TLS, który jest ułożony na szczycie pewnego niezawodnego protokołu transportowego, zwykle TCP w TCP / IP, zestawie protokołów, które uruchamiają Internet. Protokół zapisu TLS zapewnia bezpieczeństwo połączenia, które jest zarówno prywatne (przy użyciu symetrycznej kryptografii dla szyfrowania danych), jak i niezawodne (za pomocą sprawdzania spójności komunikatu). Nad protokołem zapisu TLS, zafałszowanym przez niego, znajduje się protokół uzgadniania TLS. Pozwala to serwerowi i klientowi uwierzytelniać się nawzajem, co jest główną rolą TLS w różnych formach handlu elektronicznego, takich jak bankowość internetowa. Protokół uzgadniania TLS może również negocjować algorytm szyfrowania i klucze kryptograficzne przed umieszczeniem na nim dowolnego protokołu aplikacji, takiego jak HTTP, transmituje lub odbiera swój pierwszy bajt danych

WŁAŚCIWOŚCI TLS

Zapewniając bezpieczeństwo połączeń, protokół Handshake TLS zapewnia trzy podstawowe właściwości. Tożsamość stron może zostać uwierzytelniona przy użyciu kryptografii z kluczem publicznym (takiej jak RSA). To uwierzytelnienie może być opcjonalne, ale zazwyczaj jest wymagane dla co najmniej jednej ze stron (np. Serwer Yahoo! Travel uwierzytelnia się w kliencie przeglądarki użytkownika, ale klient użytkownika nie uwierzytelnia się na serwerze Yahoo! Travel, rozróżnienie omawiane za chwilę). Drugą i trzecią podstawową cechą protokołu TLS Handshake jest to, że wspólny sekret może być bezpiecznie wynegocjowany, niedostępny dla podsłuchujących, nawet przez atakującego, który może umieścić się w środku połączenia; a negocjacja protokołu jest wiarygodna. Według słów RFC 2246: "żaden atakujący nie może modyfikować komunikacji negocjacyjnej bez wykrycia przez strony komunikacji." TLS może korzystać z różnych algorytmów szyfrowania. Dla szyfrowania symetrycznego, które jest częścią protokołu Record, można użyć DES lub RC4. Klucze tego symetrycznego szyfrowania są generowane unikalnie dla każdego połączenia i są oparte na tajnym wynegocjowanym przez inny protokół (taki jak protokół uzgadniania TLS). Protokół zapisu obejmuje sprawdzanie integralności komunikatu za pomocą klucza MAC, z bezpiecznymi funkcjami skrótu, takimi jak SHA i MD5, używanymi do obliczeń MAC. Pakiet szyfrowania używane do określonego połączenia są określane podczas początkowej wymiany między klientem a serwerem

TESTOWANIE W RZECZYWISTYM ŚWIECIE

Protokół TLS / SSL został szeroko i szeroko przetestowany w rzeczywistym świecie i został dokładnie sprawdzony przez prawdziwych kryptografów. Niektóre z ograniczeń i ograniczeń zauważone przez tych i innych ekspertów. Po pierwsze, ani dobry standard, ani dobry projekt nie gwarantują dobrego wdrożenia. Na przykład, jeśli TLS jest zaimplementowany ze słabym nasieniem losowym lub przypadkowym generatora liczb, który nie jest dostatecznie losowy, teoretyczna wytrzymałość projektu nic nie da, aby chronić dane, które są w ten sposób narażone na potencjalny kompromis. (Chociaż wykraczające poza zakres tego rozdziału, generatory liczb pseudolosowych lub PRNG odgrywają istotną rolę w wielu operacjach kryptograficznych i są zaskakująco trudne do stworzenia, chyba że dokładnie symulują prawdziwą losowość, atakujący będzie w stanie przewidzieć liczby, które generują, a tym samym pokonują każdy system, który opiera się na ich "losowej" jakości.) Drugim

ważnym zastrzeżeniem jest to, że jeśli klienci nie mają certyfikatów cyfrowych, strona klienta sesji TLS nie jest uwierzytelniana. To stwarza liczne problemy. Większość dzisiejszych "bezpiecznych" transakcji internetowych, od biletów lotniczych zarezerwowanych przez Yahoo Travel, do akcji będących przedmiotem obrotu w większości internetowych domów maklerskich, stanowi obliczone ryzyko ze strony sprzedawcy. Chociaż klient dokonujący zakupu jest zapewniony, za pomocą certyfikatu handlowca, że sprzedawca na stronie www.amazon.com naprawdę jest Amazon, sprzedawca nie ma cyfrowego zapewnienia, że komputer kliencki należy do lub jest obsługiwany przez osobę dokonanie zakupu. Oczywiście istnieją inne zapewnienia, takie jak zgodność karty kredytowej, którą kupujący dostarcza, z innymi danymi osobowymi, które pasują do niej, takimi jak adres rozliczeniowy. Ale kupiec wciąż ryzykuje zarzut i ewentualnie inne kary za nieuczciwą transakcję. W przypadku większych i bardziej wrażliwych transakcji finansowych trzeba mieć pewność, że tożsamość klienta jest większa. Certyfikat cyfrowy jest krokiem we właściwym kierunku, ale jest to krok, którego wielu kupców jeszcze nie podjęło, z kilku powodów. Pierwszy jest koszt wystawiania certyfikatów klientom, a drugim jest trudność w uzyskaniu tych certyfikatów na swoich systemach. Niektórzy kupcy zdecydowali, że koszt i wysiłek są tego warte. Na przykład Royal Bank of Scotland zastosował to podejście jego system bankowości internetowej w 1998 roku. Są inne problemy. Użytkownik musi chronić certyfikat, nawet przed takimi zagrożeniami, jak awaria sprzętu (użytkownik zmienia format dysku, traci certyfikat) lub nieautoryzowane użycie (członek rodziny korzysta z komputera i tym samym ma dostęp do certyfikatu). Ponadto użytkownik musi mieć możliwość przeniesienia certyfikatu, na przykład, na komputer przenośny, aby umożliwić dostęp do konta bankowego podczas podróży. Oczywistą odpowiedzią jest umieszczenie certyfikatu na solidnym wymiennym nośniku . Takie nośniki są ogólnie określane jako tokeny sprzętowe. Standard dotyczący tokenów jeszcze się nie pojawił. Karty inteligentne są oczywistym wyborem, ale należy wdrożyć czytniki kart. Istnieją alternatywy, takie jak umieszczanie certyfikatu na dyskietce lub na małym breloku, który podłącza się do portu USB.

KOSZT ZABEZPIECZENIA TRANSAKCJI

Dla firm, które chcą dziś wykonywać wysoce bezpieczne transakcje, korzystanie z SSL bez uwierzytelniania po stronie klienta jest krótkoterminowe, przynajmniej w przypadku niektórych kategorii transakcji. Nawet wtedy może być kosztowne, zarówno pod względem dolarów, jak i mocy obliczeniowej. Chociaż protokół TLS jest standardem otwartym, a firma Netscape dostarczyła kluczowe części technologii bez opłat licencyjnych, wciąż pozostaje pytanie, które algorytmy należy zastosować. Niektóre algorytmy są droższe od innych i nie zawsze w oczywisty sposób. Na przykład musisz licencjonować RC4, podczas gdy DES jest bezpłatny, ale RC4 jest zoptymalizowany dla 32-bitowego procesora, a DES nie. Co więcej, badania pokazują, że ilość "trafień", które może obsłużyć serwer aWeb dramatycznie spada, gdy te trafienia wymagają protokołu TLS (i znacznie spadają podczas przetwarzania uwierzytelniania klienta, a także uwierzytelniania serwera). Odpowiedź tutaj może być specjalistycznym sprzętem. Kilka firm, takich jak IBM i Rainbow Technologies, produkuje karty kryptograficzne, które zwalniają procesorowi z wyspecjalizowanego przetwarzania matematycznego związanego z kryptografią. Są tańsze niż dodawanie kolejnego serwera, aby nadążyć za bardzo wymagającym zadaniem zapewniania bezpiecznych transakcji internetowych

KOSZT ZABEZPIECZONYCH TRANSAKCJI

Dla firm, które chcą występować wysoce bezpieczne transakcje dzisiaj, używanie SSL bez uwierzytelniania po stronie klienta jest krótkoterminowe, przynajmniej w przypadku niektórych kategorii transakcji. Nawet wtedy może być kosztowne, zarówno pod względem dolarów, jak i mocy obliczeniowej. Chociaż protokół TLS jest standardem otwartym, a firma Netscape dostarczyła kluczowe części technologii bez opłat licencyjnych, wciąż pozostaje pytanie, które algorytmy należy zastosować. Niektóre algorytmy są droższe od innych i nie zawsze w oczywisty sposób. Na przykład musisz

licencjonować RC4, podczas gdy DES jest bezpłatny, ale RC4 jest zoptymalizowany dla 32-bitowego procesora, a DES nie. Co więcej, badania pokazują, że ilość "trafień", które może obsłużyć serwer aWeb dramatycznie spada, gdy te trafienia wymagają protokołu TLS (i znacznie spadają podczas przetwarzania uwierzytelniania klienta, a także uwierzytelniania serwera). Odpowiedź tutaj może być specjalistycznym sprzętem. Kilka firm, takich jak IBM i Rainbow Technologies, produkuje karty kryptograficzne, które zwalniają procesorowi z wyspecjalizowanego przetwarzania matematycznego związanego z kryptografią. Są tańsze niż dodawanie kolejnego serwera, aby nadążyć za bardzo wymagającym zadaniem zapewniania bezpiecznych transakcji internetowych.

FORMAT CERTYFIKATU X.509v3

Innym przykładem szeroko stosowanego obecnie szyfrowania komputerowego jest X.509. To nie jest statek rakietowy, ale standard dla certyfikatów cyfrowych, opisany wcześniej w tym rozdziale. Standardy X.509 Międzynarodowej Sieci Telekomunikacyjnej ds. Standaryzacji Telekomunikacyjnej (ITU-T) dokument stwierdza: "Praktycznie wszystkie usługi bezpieczeństwa są zależne od tożsamości wiarygodnych stron komunikacji, tj. uwierzytelniania." Zastanów się, w jaki sposób wpływa to na transakcje internetowe. W poprzedniej sekcji opisano, w jaki sposób SSL może szyfrować strony internetowe wysyłane z serwera WWW do klienta sieci Web i na odwrót, ale nie może zapewnić tożsamość zaangażowanych stron. Standard X.509 pomaga rozwiązać ten problem, co negatywnie wpływa na rentowność firm internetowych. Gdy użytkownik sieci internetowej prosi o zapewnienie, że strona internetowa bn.com jest rzeczywiście Barnes & Noble, może być dostarczony za pomocą certyfikatu cyfrowego . Oznacza to, że podmiot, znany jako urząd certyfikacji (CA), podjął znaczne wysiłki, aby niezawodnie zidentyfikować, a w konsekwencji poświadczać, że akceptant jest prawowitym właścicielem klucza szyfrującego. Ten klucz jest publiczną połową unikatowej i matematycznie powiązanej pary kluczy publiczny / prywatny, tak że wiadomość zaszyfrowana za pomocą klucza publicznego może zostać odszyfrowana tylko za pomocą odpowiedniego klucza prywatnego. Osoby fizyczne, a także sprzedawcy mogą mieć parę kluczy publiczny / prywatny. Bank może wówczas uzyskać dostęp do tego klucza publicznego i użyć go oraz klucza prywatnego banku, aby zaszyfrować dane konta, które wysyła do klientów przez Internet. Tylko klient z odpowiednim kluczem prywatnym może odszyfrować te informacje, korzystając z klucza publicznego banku. Jednocześnie klienci wiedzą, że informacja może pochodzić tylko z banku (w przeciwnym razie klucz publiczny banku nie działałby w celu odszyfrowania go). Klienci wiedzą również dzięki zaszyfrowanej wiadomości (cyfrowy odcisk palca treści wiadomości), że dane, które otrzymują z banku, nie zostały zmienione. W związku z tym bardzo trudno jest twierdzić, że żadna ze stron nigdy nie miała miejsca. W ten sposób cyfrowe certyfikaty mogą się poprawić poufność, integralność i nieodrzucanie.

ISO / IEC / ITU 9594-8 a.k.a. X.509.

Zarządzanie publicznymi kluczami to zadanie infrastruktury klucza publicznego (PKI), którego istotnym elementem jest standard X.509. Na przykład pracownicy organizacji mogą wykonywać bezpieczną komunikację biznesową przez Internet, np. Negocjacje kontraktów, za pomocą PKI. Aby zaangażować się w bezpieczną transakcję z kimś, konieczne jest znalezienie i dostęp do klucza publicznego drugiej osoby i na odwrót. Odpowiedź brzmi: publikuj klucze publiczne w formie certyfikatu cyfrowego, a następnie użyj jakiejś formy katalogu, aby je zlokalizować. Aby umożliwić współpracę różnych systemów, opracowano standardy dla katalogów, w szczególności X.500. Norma ta stosuje takie elementy standaryzacji katalogów jak hierarchiczna konwencja nazewnictwa:

Kraj, organizacja, nazwa zwyczajowa.

Więc Fred Jones z Megabank może mieć nazwę X.500:

[Country = US, Organization = Megabank, Inc., Common Name = Fred Jones]

Sposób lokalizowania certyfikatów cyfrowych w celu weryfikacji tożsamości był logicznym rozszerzeniem standardu, dlatego opracowano X.509, oficjalnie znany jako ITU-T X.509 (dawniej CCITT X.509), a także ISO / IEC / ITU 9594-8 . W X.509 znajduje się definicja podstawowego formatu certyfikatu, który składa się z siedmiu pól pokazanych w Załączniku 7.19. Format certyfikatu znacznie się rozwinął od 1988 roku. Oryginalny format to teraz określane jako X.509v1. Po zmianie wersji X.500 w 1993 r. Dodano dwa dodatkowe pola do obsługi kontroli dostępu do katalogów, co skutkowało formatem X.509v2. X.509v2 dodał unikalne identyfikatory dla emitenta i podmiotu, opcjonalne ciągi bitowe używane do wydania emitenta i jednoznaczne nazwy podmiotów w przypadku późniejszego przypisania tej samej nazwy do różnych podmiotów. Załóżmy, że Fred Jones, którego nazwisko X.500 zostało nadane wcześniej, jest wiceprezesem zarządu Megabank, a następnie zostaje wynajęty przez konkurenta. Megabank odrzuca jego imię, ale jeśli inny Fred Jones, programista, następnie przychodzi do pracy dla Megabanku, zostaje skutecznie przypisany do tej samej nazwy X.500:

[Country = US, Organization = Megabank, Inc., Common Name = Fred Jones]

Powoduje to problemy z autoryzacją dla jakichkolwiek list kontroli dostępu dołączonych do obiektów danych X.500, ze względu na trudność zidentyfikowania wszystkich list kontroli dostępu, które nadają uprawnienia konkretnemu imieniu użytkownika. Unikatowe pole identyfikatora dodane w X.509v2 zapewnia możliwość wstawienia nowej wartości za każdym razem, gdy nazwa jest ponownie używana. W rzeczywistości lepszym rozwiązaniem jest użycie lepszego wyróżnika w nazwie X.500, takiego jak:

[Common Name = Fred Jones, Employee Number = 1000002]

W 1993 r., Kiedy opublikowano dokumenty RFC dotyczące ochrony prywatności w Internecie (PEM), zawierały one specyfikacje infrastruktury klucza publicznego opartej na certyfikatach X.509v1. Próby wdrożenia PEM ujawniły jednak braki w formatach certyfikatów w wersji 1 i 2. W konsekwencji, ISO / IEC / ITU i ANSI X9 opracowały format X.509v3 , który znacznie rozszerza możliwości formatu, udostępniając pola rozszerzeń i szersze opcje nazywania w X.509v3.

ROZSZERZENIE STANDARDU

Rozszerzenia zostały dodane w wersji 3 aby rozwiązywać problemy wykryte podczas wdrażania certyfikatów wersji 1 i 2. Poszczególne typy pól rozszerzeń mogą teraz być określone w standardach lub zdefiniowane i zarejestrowane przez dowolną organizację lub społeczność. Każde pole rozszerzenia jest przypisywane typowi za pomocą identyfikatora obiektu, zarejestrowanego w taki sam sposób, jak zarejestrowany jest algorytm. Chociaż teoretycznie każdy może zdefiniować typ rozszerzenia, aby osiągnąć praktyczną interoperacyjność, wspólne typy rozszerzeń muszą być zrozumiane przez różne implementacje. Dlatego najważniejsze typy rozszerzeń są ustandaryzowane. Ale gdy X509v3 jest używany w zamkniętej grupie - na przykład grupie partnerów biznesowych - możliwe jest zdefiniowanie unikatowych typów rozszerzeń w celu zaspokojenia określonych potrzeb.

ŹRÓDŁA, PROBLEMY I URZĘDZY CERTYFIKACJI X.509

Ktoś zarządzający projektem e-commerce niekoniecznie musi znać X.509 w szczegółach, ale powinien przynajmniej przeczytać dokument Arsenault i Turner; wyraźnie opisuje nie tylko X.509, ale rolę, jaką odgrywa w PKI (które określają jako "zestaw sprzętu, oprogramowania, ludzi, zasad i procedur") potrzebne do tworzenia, zarządzania, przechowywania, dystrybucji i odwoływania certyfikatów opartych na kryptografii z kluczem publicznym "55). Bardzo pomocne są również prezentacje autorstwa VeriSign'sWarwick Ford, które NIST ma online na stronie itsWeb. Dla programisty e-commerce, który chce więcej szczegółów, kolejnym krokiem jest książka Forda, napisana wspólnie z

innym wykonawcą VeriSign Michaelem Baumem, Secure Electronic Commerce.56 Dokumentuje to inne ważne aspekty X.509, takie jak lista odwołań certyfikatów, używana do odwołać certyfikaty przed ich wygaśnięciem (np. jeśli klucz prywatny został naruszony). Dostępna jest także kopia standardu, dostępnego online, na stronie internetowej Międzynarodowej Unii Telekomunikacyjnej (ITU) (www.itu.int). Rozszerzenia i ulepszenia w formacie certyfikatu X.509v3 znacznie się zwiększają jego użyteczność, ale zapewnienie jednolitej metody wychodzenia poza standard podnosi widmo braku standaryzacji. Jest to kwestia, którą zajmuje się grupa PKIXworking IETF. Są też inne kwestie, które należy wziąć pod uwagę przy ocenie X.509 jako technologii bezpieczeństwa, z których wiele podnosi Ed Gerck z Meta-Certificate Group. Artykuły na stronie internetowej grupy zwracają uwagę, że X.509 nie odnosi się do "poziomu wysiłku, który jest potrzebny do sprawdzenia poprawności informacji w certyfikacie". Innymi słowy, niektóre problemy bezpieczeństwa wykraczają poza zakres X.509, ale muszą być brane pod uwagę przy wdrażaniu systemów opartych na tych certyfikatach. Na przykład nie ma sensu polegać na certyfikacie cyfrowym, jeżeli środki podjęte w celu zapewnienia tożsamości właściciela i użytkownika certyfikatu nie są współmierne do ryzyka związanego z poleganiem na certyfikacie. Ponadto transakcje, które nie używają certyfikatów po obu stronach pozostaną z natury problematyczne. Te problemy wskazują na znaczenie roli odgrywanej przez CA. Jak wspomniano wcześniej, urzędy certyfikacji są podmiotami, które wystawiają i podpisują certyfikaty. Każdy ma klucz publiczny, który jest wymieniony w certyfikacie. Urząd odpowiedzialny jest za zaplanowanie daty wygaśnięcia i cofnięcie certyfikatów w razie potrzeby. Urząd certyfikacji utrzymuje i publikuje listę odwołania certyfikatów (CRL). Innymi słowy, zapewnienie ważności certyfikatów wymaga wielu czynności konserwacyjnych. CRL, na przykład, ma kluczowe znaczenie, jeśli certyfikaty zostały naruszone lub stwierdzono, że zostały wydane w nieuczciwy sposób. Stało się tak w 2001 roku, kiedy okazało się, że kilka certyfikatów VeriSign zostało wydanych przez pomyłkę osobie udającej Microsoft. Ponieważ niektórzy użytkownicy komputerów polegają teraz na certyfikatach w celu zagwarantowania autentyczności aktualizacji oprogramowania i komponentów, niezapoznanie się z listą odwołania przed pobraniem certyfikowanego kodu może spowodować złośliwe ataki. Problemy z certyfikatami mogą mieć szeroki wpływ, ponieważ uprawnienia w certyfikatach są hierarchiczne. Kiedy urząd certyfikacji wystawia certyfikat, podpisuje go swoim własnym kluczem. Każdy, kto powołuje się na certyfikaty wydane przez ten urząd certyfikacji, musi wiedzieć, przez jakie organy wystawia ten certyfikat. Aby uprościć, istnieją dwie możliwe odpowiedzi. Urząd certyfikacji sam się poświadcza, tj. Udostępnia własny klucz "root" lub korzysta z innego urzędu certyfikacji dla klucza głównego. Najwyraźniej każdy kompromis związany z kluczem głównym podważa wszystkie certyfikaty, które zyskują na nim uprawnienia.

POZA RSA I DES

Badania i rozwój kryptografii nie zakończyły się wraz z rozwojem algorytmów RSA. Wydarzenia w ostatnich dwóch dekadach XX wieku i pierwszej dekadzie XXI wieku oraz ich implikacje omówiono w ostatniej części rozdziału, która kończy się ostrzeżeniami wdrażanie szyfrowania.

KRYTPOGRAFIA KRZYWEJ ELIPTYCZNEJ

W 1985 roku Neal Koblitz z University of Washington i Victor Miller z IBM niezależnie odkryli zastosowanie systemów krzywych eliptycznych do kryptografii. W przypadku zastosowania do kryptografii z kluczem publicznym, arytmetyka krzywej eliptycznej ma pewne zalety w stosunku do technik klucza publicznego pierwszej generacji, takich jak Diffie-Hellman i RSA. Bezpieczeństwo algorytmów krzywych eliptycznych opiera się na tej samej zasadzie, co algorytm Diffiego-Hellmana, dyskretny problem z logami, jak opisano w rozdziale 7.4.2. Zalety algorytmów krzywych eliptycznych leżą w wielkości klucza potrzebnej do osiągnięcia pewnych poziomów bezpieczeństwa. Wraz z podnoszeniem bezpieczeństwa w miarę upływu czasu, aby sprostać ewoluującemu zagrożeniu ze

strony podsłuchujących i hakerów z dostępem do większych zasobów obliczeniowych, krzywe eliptyczne zaczynają dawać ogromne oszczędności w stosunku do starych technik pierwszej generacji. Do roku 2010 systemy kluczy publicznych używały 1024 bitów lub 2048 bitów do tworzenia kluczy. Firma NIST zaleciła, aby po 2010 roku systemy te zostały zaktualizowane do systemu, który zapewni odpowiednie zabezpieczenia. Jednym ze sposobów jest zwiększenie rozmiaru klucza, który jest używany. Jednak systemy, które są obecnie na miejscu, stają się coraz bardziej kłopotliwe, im większy jest kluczowy rozmiar. NSA zatwierdza kryptografię krzywych eliptycznych, podając na swojej stronie internetowej, że zaimplementowała systemy kryptografii z kluczem publicznym w formie krzywych eliptycznych, aby chronić zarówno informacje klasyfikowane, jak i niesklasyfikowane.59 Systemy krzywych eliptycznych są sposobem na umiarkowany wzrost rozmiaru klucza, gdy wymagane jest większe bezpieczeństwo .Tak więc, aby użyć RSA do ochrony 256-bitowego klucza AES, należy użyć klucza 15,360 bitów, czyli o rząd wielkości większych niż kluczowe rozmiary obecnie używane w Internecie. Jednak eliptyczny klucz krzywej musiałby wynosić tylko 521 bitów. Algorytmy krzywych eliptycznych mogą wykorzystywać mniejsze klawisze, ponieważ zaangażowana matematyka sprawia, że operacja odwrotna, lub odszyfrowywanie, jest trudniejsza wraz ze wzrostem długości klucza. Inną cechą, która sprawia, że krzywe eliptyczne są atrakcyjne, jest fakt, że są one bardziej wydajne niż obecne implementacje kryptografii klucza publicznego, które wydają się być stosunkowo powolne, co powoduje, że są one wykorzystywane bardziej jako kluczowe metody dystrybucji niż metody szyfrowania danych.

WYGAŚNIĘCIE PATENTU RSA

6 września 2000 r. firma RSA Security opublikowała publiczny algorytm szyfrowania RSA w publicznej domenie. Oznacza to, że każdy może teraz tworzyć produkty, które zawierają ten algorytm (pod warunkiem, że jest to jego własna implementacja, a nie jedna licencja z RSA). W efekcie RSA Security zrezygnowała z prawa do wyegzekwowania patentu na wszelkie działania rozwojowe, które obejmują algorytm RSA występujący po 6 września 2000 r. Patent amerykański dla algorytmu RSA wygasł 20 września 2000 r. W rezultacie uzyskano jeszcze szersze zastosowanie szyfrowania kluczem publicznym, po niższych kosztach. Patent RSA był zawsze nieco kontrowersyjny, ponieważ dotyczył matematyki, która nie jest tym, co większość ludzi myśli, gdy myślą o wynalazku. Właściciele patentu nigdy nie byli w stanie rozszerzyć ochrony poza Stany Zjednoczone. W rezultacie, wersje szyfrowania klucza publicznego oparte na alternatywach algorytmu RSA zostały opracowane i sprzedane poza granicami kraju przez firmy, takie jak Baltimore Technologies w Irlandii, F-Secure w Finlandii i Israel Algorithmic Research. Teraz firmy szyfrujące mogą zrezygnować z kosztownej obsługi wielu wersji swoich produktów o kluczu publicznym (w USA i poza USA). Ponadto firmy z USA mogą opracowywać i sprzedawać produkty oparte na RSA. Duże firmy faktycznie mogą "przetworzyć własne" schematy szyfrowania klucza publicznego do użytku wewnętrznego, na podstawie sprawdzonego, wolnego od opłat algorytmu.

DES ZASTĄPIONY

RSA Security, firma, która próbowała uczynić algorytm RSA synonimem szyfrowania kluczem publicznym, odegrała wiodącą rolę w drugim przełomowym wydarzeniu kryptograficznym z 2000 roku, nazwanie następcy DES, standardu szyfrowania danych. Jak wspomniano wcześniej, projekty takie jak EFF DES Cracker wykazały, że komputer zbudowany za mniej niż 250 000 USD może odszyfrować wiadomość zaszyfrowaną DES w mniej niż trzy dni. W rzeczywistości było to częścią "DES Challenges" sponsorowanych przez RSA Security. DES Challenge Wygrał Rocke Verser z Loveland w stanie Kolorado, który poprowadził grupę użytkowników Internetu w rozproszonym ataku z użyciem brutalnej siły. Projekt o nazwie kodowej DESCHALL, rozpoczęło się 13 marca 1997 r. i zakończyło się sukcesem około 90 dni później. DES Challenge II składał się z dwóch konkursów opublikowanych 13 stycznia i 13 lipca

1998 roku. Pierwszy konkurs został złamany przez rozproszoną pracę obliczeniową koordynowaną przez distributed.net, który sprostał wyzwaniu za 39 dni. Drugi konkurs został rozwiązany przez specjalnie zaprojektowany DESF DES Cracker. Efektem tych projektów było zwrócenie uwagi na potrzebę silniejszego szyfrowania. Firmy i agencje rządowe, które chcą archiwizować poufne dane, muszą zachować bezpieczeństwo przez dziesięciolecia, a nie dni. Jednak, jak przewidywano w latach siedemdziesiątych, postępy w dziedzinie zasilania komputerów sprawiły, że "przestarzały" był DEA, szeroko stosowany algorytm klucza prywatnego, który tworzy podstawą DES. Oczywiście termin "przestarzały" jest w tym kontekście względny. DES nie jest przestarzały, gdy aplikacje muszą szyfrować dane masowe, aby zachować poufność przez ograniczony czas, a wiele danych należy do tej kategorii. W 1997 r. Rząd USA rozpoczął proces ustanawiania bardziej wydajnego standardu niż DES, znanego jako Advanced Encryption Standard (AES). Jest to publikacja FIPS (Federal Information Processing Standard), FIPS 197, określająca "algorytm kryptograficzny do użytku przez organizacje rządowe USA w celu ochrony wrażliwych (niesklasyfikowanych) informacji." Rząd przewidywał prawidłowo, że AES będzie "Szeroko stosowane na zasadzie dobrowolności przez organizacje, instytucje i osoby spoza rządu Stanów Zjednoczonych - i poza Stanami Zjednoczonymi - w niektórych przypadkach." W istocie, przeprowadzono konkurs, aby znaleźć najlepszy możliwy algorytm dla danego zadania, oraz Zwycięzcą, wybranym w październiku 2000 r., był Rijndael (wymawiane "Ren Doll"). Algorytm ten został opracowany specjalnie dla AES przez dwóch kryptografów z Belgia, dr Joan Daemen i dr Vincent Rijmen. Rijndael jest szyfrem blokowym o zmiennej długości bloku i długości klucza. Jak dotąd, klucze o długości 128, 192 lub 256 bitów zostały określone do szyfrowania bloków o długości 128, 192 lub 256 bitów. (Możliwe są wszystkie dziewięć kombinacji długości klucza i długości bloku.) Jednakże zarówno długość bloku, jak i długość klucza można bardzo łatwo rozszerzyć w wielokrotnościach 32-bitowych. Rijndael można wdrożyć bardzo wydajnie w sprzęcie, nawet na kartach inteligentnych.

KRYPTOGRAFIA KWANTOWA

Nowa podstawa obliczeń głęboko wpłynie na siłę kryptograficzną w nadchodzących dziesięcioleciach. Ta sekcja zawiera krótkie i nietechniczne podsumowanie nauki o obliczeniach kwantowych i kryptografii kwantowej.

PERSPEKTYWA HISTORYCZNA

Skupiamy się na statusie kryptografii, jaki obecnie istnieje. Klasyczny komputer był wystarczający do wykonywania obliczeń i procesów wymaganych od AES, RSA i wszystkich systemów kryptograficznych i algorytmów, które były badane od czasu pojawienia się kryptografii. Chociaż współczesne komputery są zasadniczo takie same jak w latach 50. XX wieku, maszyny, których używamy dzisiaj, są znacznie szybsze. Mimo że szybkość wzrosła, podstawowe zadanie komputerów pozostało niezmienione: "manipulować i interpretować kodowanie bitów binarnych w użyteczny wynik obliczeniowy." Aby przesunąć granice wydajności komputera kiedykolwiek, cel naukowców komputerowych " było zmniejszenie rozmiarów tranzystorów używanych we współczesnych procesorach. "Wczesne komputery były zbudowane z bram i magazynów" bitów "wykonanych z wielu tysięcy cząsteczek. Składniki dzisiejszych procesorów poruszają się w kierunku kilkuset cząsteczek. Przemysł komputerowy zawsze wiedział, że miniaturyzacja osiągnie barierę, poniżej której nie można zbudować obwodów, ponieważ zmieniłoby się ich podstawowe fizyczne zachowanie. Komponenty nowoczesnych komputerów sięgają tej bariery; gdyby tranzystory stały się znacznie mniejsze, "ostatecznie osiągną punkt, w którym pojedyncze elementy nie będą większe niż kilka atomów". Informatycy obawiają się tego ciągłego kurczenia się, ponieważ na poziomie atomowym prawa mechaniki kwantowej będą regulować właściwości i zachowanie obwodów, a nie prawa mechaniki klasycznej. Nauka mechaniki kwantowej nie jest w pełni zrozumiała dla naukowców; początkowo uważano, że jest to istotne ograniczenie ewolucji technologii komputerowej. Dopiero w 1982 r. Społeczność naukowa dostrzegła

korzyści wynikające z niezwykłych efektów mechaniki kwantowej. W tym samym roku Richard Feynman wysunął teorię na temat nowego typu komputera, który wykorzystałby efekty mechaniki kwantowej i wykorzystał te efekty na swoją korzyść69. W 1985 r. David Deutsch z University of Oxford opublikował "przełomowy teoretyczny artykuł opisujący jak proces mógłby być doskonale modelowany (teoretycznie) za pomocą kwantowego systemu komputerowego. Dalej dowodził, że system kwantowy byłby w stanie wykonywać zadania, których nie mógłby wykonać żaden nowoczesny komputer, na przykład generowanie prawdziwych liczb losowych. "Po tym, jak Deutsch opublikował ten artykuł, poszukiwania zaczęły znajdować interesujące zastosowania dla takiej maszyny".

PODSTAWY

Mechanika kwantowa wyjaśnia fizykę i zachowania cząstek, atomów i energii. Pomysł komputera kwantowego opiera się na zjawiskach doszło na poziomie atomowym i subatomowych, które są wyjaśnione "przez mechaniki kwantowej i klasycznej Defy wszystkie prawa fizyki. Zjawiska te zostaną wkrótce omówione bardziej szczegółowo; W tym miejscu należy jednak wyjaśnić kilka podstawowych różnic między klasycznymi współczesnymi komputerami a ideą komputera kwantowego. Klasyczne komputery przechowują i przetwarzają informacje w jednostkach zwanych bitami, reprezentowanych jako zero (0) lub jeden (1) w tranzystorze komputera. Bity są następnie ułożone w bajty, szereg ośmiu bitów. W ten sposób informacje przechowywane na komputerze są przechowywane jako pojedyncze bity. Dlatego dokument jest "jednym z dwóch różnych stanów" i nie jest przeznaczony do używania w odniesieniu do konkretnego komputera. a '0' lub '1'. "77 To prowadzi do pierwszej różnicy między klasycznymi komputerami a komputerami kwantowymi. Quantum komputery przechowywania i przetwarzania informacji w jednostkach nazywanych bity kwantowe, określane przez mianem "qubitach." "Qubity reprezentuje atom jony, fotony lub elektrony i ich urządzeń sterujących respectivement nie pracują razem, aby działać jako pamięci komputera i procesora." Podobny do klasyczny bitowe qubit jest reprezentowany jako 0 lub 1. w przeciwieństwie do klasycznej bitowe qubit mogą zatem istnieć w superpozycji Zarówno 0 i 1. innymi słowy, jest to możliwe dla jednego qubit istnieć jako 0, a 1, lub jednocześnie zarówno jako 0 a 1. qubit nie znajduje się w dwóch położeniach na raz mówi się, że w stan koherentny. To może być wyjaśnione "bardziej spójnie co przykład: Jeżeli moneta jest obrócony w ciemnym pomieszczeniu, w wyniku monety są odwrócone jest matematycznie podobnie jak głowy i ogony. Gdy światło jest wyłączone, moneta znajduje się w superpozycji - jest to jednocześnie głowa i ogon, ponieważ w obserwatorze nie można zobaczyć, która to jest. Jeśli [obserwator] włączy światło, "zapadnie" superpozycja i zmusi monetę do zmierzenia głowami lub ogonami. Pomiar czegoś niszczy superpozycję, zmuszając ją do istnienia właśnie w stanie klasycznym. Byłoby to potężniejsze niż jakikolwiek komputer do tej pory; Zasadniczo, ponieważ kubit w stanie koherentnym zawiera dwie wartości naraz, pojedynczą operację wykonaną w tym samym czasie. Podobnie, system z dwoma kubitami wykona operację cztery wartości i trzykubitowy system na ośmiu [wartościach]. "Podsumowując, operacja wykonana na systemie kubitów działałaby jednocześnie na wartościach 2^n

Aby wykorzystać moc paralelizmu kwantowego, "własność, która sprawia, że obliczenia kwantowe są tak potężne, jest bardzo delikatna i trudna do kontrolowania". Naukowcy muszą być w stanie odczytać i zmierzyć wynik z operacji wykonywanych na grupach kubitów. Wprowadź problem dekoherencji. Kiedy qubit w stan koherentny wymiernie wzajemnych aktów z otoczeniem, to natychmiast wznowić deco tu i jeden z dwóch stanów klasycznych, albo 0 albo 1, i nie będzie już wykazywać zdolność podwójnego państwa. Innymi słowy, samo patrzenie na kubit może spowodować jego dekodowanie, co uniemożliwia pomiar kubitów. Jeśli naukowcy nie będą chcieli zmierzyć czegoś bezpośrednio, wtedy nie zostaną stworzeni. Jedna możliwa odpowiedź leży w innej własności mechaniki kwantowej zwanej splątaniem. Splątanie jest niejasnym atrybutem, który obejmuje dwa lub więcej atomów lub cząstek.

Gdy spełnione są określone warunki, mogą się zaplątać. W splątane cząstki pozostanie uwikłany, bez względu na fizyczną odległość między nimi, a jeden splątanych cząstek zawsze będzie w stanie komunikować się ze swoim partnerem. Cząsteczki wirują w górę lub w dół i tak naukowcy mierzą informacje o cząstkach. Nieruchomość koherencji mówi nam czy cząstka będzie spin zarówno w górę Równocześnie iw dół aż naukowiec patrzy na niego i środków niej. Stan wirowania mierzonej cząstki wynosi. , , przekazywane do skorelowanej cząstki, która jest przeciwnym kierunkiem wirowania niż kierunek mierzonej cząstki. "W ten sposób uwikłanie może pozwolić naukowcom na poznanie wartości kubitu bez patrzenia na niego. Naukowcy przyznają, że uwikłanie to trudne pojęcie; wciąż eksplorują tę koncepcję rozwiązuje się praktyczne rozwiązanie problemu pomiaru informacji w systemie kwantowym.

ODDZIAŁYWANIA

Chociaż teoretycznie kwantowe komputery mogą wykonywać dowolne zadania, nie musi to oznaczać komputera. Mnożenie jest często cytowanym przykładem czegoś, co można zrobić równie szybko, jak komputer komputer kwantowy. Od wczesnych etapach informatyki kwantowej, naukowcy wiedzieli tak aby wykazać najwyższą moc obliczeniową, nowe algorytmy będą musiały być zaprojektowane, aby wykorzystać zjawisko równoległości kwantowej. Algorytmy przeszukiwania są skomplikowane i trudne do zaprojektowania, ale dwa z nich napędzają rozwój wysoce teoretycznego pola: algorytmu Shora i algorytmu Grover'a. Peter Shor z Bell Labs przeznaczony pierwszy w 1994 roku algorytm kwantowy algorytm faktoryzacji shora pozwala na szybkie faktoringu bardzo dużych liczb do swoich głównych czynników. Na przykład, naukowe szacunki mówią, że zajęłoby to nowoczesnemu komputerowi 1024 lat rozkład na czynniki 1000-cyfrowej liczby; zajęłoby to komputer kwantowy około 20 minut. Implikacje tego algorytmu kwantowego dla klasycznych algorytmów, które zależą od trudności faktoryzacji dla bezpieczeństwa, takich jak szeroko stosowany algorytm RSA, są ogromne. Lov Grover, znany również jako Bell Labs, wynalazł drugi algorytm kwantowy w 1996 roku. Algorytm Grover'a pozwala komputerowi kwantowemu na szukanie znacznie więcej szybka niż jakakolwiek istniejąca dziś zdolność. Grover zauważa, że największą korzyść uzyskuje się, gdy jego algorytm jest używany w nieposortowanej bazie danych. Średnio zajmuje klasyczny numer komputera. Algorytm Grover pozwala zrobić to samo w pierwiastku kwadratowym z n liczbą wyszukiwań. Na przykład w bazie danych zawierającej 1 milion wpisów, dzisiejszy komputer potrzebuje średnio 500 000 wyszukiwań. zajmie to komputer kwantowy, używając algorytmu Grover'a tylko 1000 wyszukiwań. Może to mieć wpływ na klucz symetryczny algorytmy: takie jak DES, ponieważ algorytm pozwoli na wyczerpującym poszukiwaniu wszystkich możliwych kluczy nastąpić dość szybko

OBECNY STATUS

Stany Zjednoczone mają wiele inicjatyw w toku, Stany Zjednoczone mają wiele inicjatyw w ruchu. W 2001 r. Agencja Obrony Zaawansowanych Projektów Badawczych (DARPA) Departamentu Obrony zainwestowała 100 milionów dolarów w wysiłek, który potrwa pięć lat. Ponadto, National Science Foundation ma 8 milionów dolarów w postaci pieniędzy z grantu na badania zdolności kwantowych. Inicjatywa Quantum Information Science and Technology DARPA chce istnieć w nieskończoność; 2006.96 Wiele innych rządów, głównie w Europie i Azji, bierze udział w badaniach i rozwoju kwantowych obliczeń. W 2000 r. Komisja Europejska zainwestowała 20 milionów dolarów w budżecie na trzy lata kompleksowego wysiłku badawczego. W Japonii, Ministerstwo Poczty i Telekomunikacji rozpoczął inicjatywę w 2001 thatwill obciążenie 10 lat z o łącznym budżecie wynoszącym $ 400 milionów dolarów. W projektach kwantowych zaangażowanych jest kilka przedsiębiorstw komercyjnych. Obejmuje to firmy IBM, Bell Labs, japońskie firmy Fujitsu, Ltd., NEC Corporation oraz Nippon Telephone and Telegraph Corporation .Ta lista nie jest wyczerpująca, istnieją uniwersytety i inne organizacje na całym świecie. Ze względu na ogólnoświatową próbę lepszego zrozumienia

obliczeń kwantowych dokonano kilku kluczowych postępów. W 1998 roku naukowcy z Los Alamos National Laboratory i MIT mogli omówić quiz dotyczący trzech spinów jądrowych pewnych typów cząsteczek. Zgodnie z eksperymentami, rozprowadzanie informacji (kubit) na zewnątrz sprawiło, że trudniej jest ją zepsuć lub zdekoncentrować. Badacze byli w stanie tego dokonać za pomocą techniki zwanej jądrowego rezonansu magnetycznego (NMR), który pozwala na manipulację i kontrolę wirowania jądro ma. Ta technika służy do analizy informacji kwantowej. W 2000 r. Naukowcy z IBM opracowali komputer pięciokubitowy, czyli wykorzystujący jądra cieczy. Jądra zostały zaprogramowane za pomocą impulsów o częstotliwości radiowej, a następnie wykryte za pomocą technik NMR. Korzystając z tej techniki, zespół jest w stanie znaleźć okres określonej funkcji lub długość najkrótszego przedziału, w którym powtarza swoje wartości. Ten problem wymagałby wykonania kilku czynności; zespół w IBM, co robić w jednym kroku. W 2001 roku połączona grupa naukowców z IBM i Uniwersytetu Stanforda demostrated algorytm Shor i były zdolne do znalezienia głównych czynników 15. Komputer siedmiu qubit Prawidłowo wydedukować zrobił głównymi czynnikami były 3 i 5,99 w lutym 2007 roku kanadyjska firma o nazwie D-Wave twierdził, że to demonstruje pierwszy komercyjny komputer kwantowy. Jest to "supercoolowany, nadprzewodnikowy niobowy chip zawierający 16 kubitów." 100 D-Wave nie skupia się na wysiłkach kryptograficznych podczas budowy Oriona, jak nazywa się komputer. Zamiast tego Orion koncentruje swoją energię na rozwiązywaniu problemów związanych z dopasowywaniem wzorców i niedeterministycznym wielomianem problemy (problemy NP-zupełne). Problemy NP-zupełne są zawarte w rozwiązaniu pewnego problemu. Przykłady takich problemów obejmują wyszukiwanie w bazie danych, dopasowywanie wzorców, identyfikowanie chorób na podstawie objawów oraz znajdowanie dopasowań do materiału genetycznego. Demonstracje firmy zostały przeprowadzone za pomocą kanału telewizyjnego z odległej lokalizacji, ze względu na delikatny charakter maszyny w sprzęcie transportowym, która jest chłodzona do poziomu powyżej zera bezwzględnego. Pomimo demonstracji i roszczeń D-Wave, naukowcy są sceptyczni, że Orion faktycznie wykonuje obliczenia kwantowe. Nawet dyrektor generalny D-Wave powiedział, że chociaż Orion wykonuje obliczenia kwantowe, jest pewna niepewność. Niemniej jednak, D-Wave ogłosiła plany zwiększenia Orion 1000 qubitach roku 2008. W lipcu 2007 roku, naukowcy z NIST (Stany Zjednoczone) i Rutherford Appleton Laboratory (Wielka Brytania) połączyły siły, aby zbadać efekty kwantowe magnetyczne. To 100 atomów niklu itru i baru do kwantowego łańcucha spinowego, które w efekcie zamieniają cząsteczkę magnetyczną o długości 30 nanometrów w pojedynczy element. "To odkrycie jest ważnym krokiem w kierunku postawienia kubitów na obwody półprzewodnikowe. Trzydzieści nanometrów wykracza daleko poza skalę długości atomowej i niecodziennie jest widzieć koherencję kwantową poza poziomem atomowym. Jednak zespół zgłosił stabilne stany koherentne w tej wielkości, która jest wystarczająco duża dla technik litograficznych stosowanych do tworzenia płytek obwodów i przewodników klasycznych komputerów. W kwietniu 2013 roku, naukowcy "z powodzeniem trans mitted bezpieczny kod kwantową przez atmosferę z do samolotu do stacji naziemnej." Autor kontynuuje: "To pokazuje nie kryptografia kwantowa może być realizowane w celu rozbudowy istniejących systemów", mówi LMU Sebastian Nauerth. W eksperymencie wysłano pojedyncze fotony samolot do odbiornika na ziemi. Wyzwanie dla fotonów może być skierowane na teleskop na ziemi pod wpływem wibracji mechanicznych i turbulencji powietrza. Florian Moll, kierownik projektu w Instytucie Łączności i Nawigacji DLR, donosi: "Przy pomocy szybko poruszających się lusterek, precyzja celowania jest mniejsza niż 3 m na odcinku 20 km", informuje Florian Moll. Przy takim poziomie dokładności William Tell mógł trafić jabłko na głowę syna nawet z odległości 500 metrów. Związek między nimi a efektami turbulencji powietrza, warunki napotkane podczas eksperymentu były porównywalne. To samo dotyczy prędkości kątowej samolotu. Sukces eksperymentu stanowi zatem ważny krok w kierunku bezpiecznej globalnej komunikacji satelitarnej. Z tymi właśnie wskazówkami sceptycy są przekonani, że praktyczne komputery kwantowe to jeszcze lata, a nawet dziesięciolecia. Po przeprowadzeniu wielu godzin badań na temat obliczeń kwantowych autor

uważa, że nie jest to kwestia obliczeń kwantowych. Naukowcy byli w stanie wykazać kilka obliczeń kwantowych na systemach Jednak naukowcy muszą pokonywać wiele przeszkód. Do wykonywania użytecznych obliczeń potrzebne będą systemy zawierające setki lub tysiące kubitów. Ponadto wymagane są precyzyjne kontrole w celu wykonania operacji przy jednoczesnym uniknięciu dekoherencji; w rzeczywistości dekoherencja jest prawdopodobnie największą przeszkodą w stworzeniu systemu kwantowego

CZYNNIK PANACEUM

Ponieważ dostawcy oprogramowania szyfrującego i kryptografowie zajmują się implementacją i rozszerzonymi testami nowych algorytmów, ważne jest, aby zwrócić uwagę na te słowa z wymagań konkurencji AES: Należy dołączyć pełną pisemną specyfikację algorytmu, składającą się z wszystkich niezbędnych równań matematycznych, tabel , schematy i parametry potrzebne do implementacji algorytmu. Innymi słowy, nie ma tajemnicy na temat tego, w jaki sposób AES utwierdzi sprawy w tajemnicy, tak jak nie ma tajemnicy na temat działania DES. Często uderza to nowicjusza jako nielogiczne. Dlaczego nie utrzymasz algorytmu w tajemnicy? Z pewnością spowoduje to, że wszystkie wiadomości zaszyfrowane za pomocą tego narzędzia będą znacznie trudniejsze do odszyfrowania. Nie całkiem. Wszelkie poleganie na tajemnicy algorytmu wstawia słabe ogniwo w łańcuchu bezpieczeństwa. Szyfrowanie danych nie gwarantuje, że pozostanie poufne. Klucze należy zachować w tajemnicy, a tożsamość osób ubiegających się o upoważniony dostęp musi zostać zweryfikowana, aby upewnić się, że są one autentyczne i tak dalej. Dotyczy to zarówno szyfrowania kluczem publicznym, jak i szyfrowania kluczem prywatnym. Zasada ta jest znana jako Zasada Kerckhoffa, oparta na publikacji z 1883 roku przez wojskowego kryptologa Auguste Kerckhoffsa:

1. System musi być praktycznie, jeśli nie matematycznie, nieczytelny;

2. Nie można wymagać, aby był tajny i musi być w stanie wpaść w ręce wroga bez żadnych niedogodności;

3. Jego klucz musi być komunikatywny i możliwy do utrzymania bez pomocy pisemnych notatek, a także zmienny lub modyfikowalny wbrew woli korespondentów;

4. Musi mieć zastosowanie do korespondencji telegraficznej;

5. Musi być przenośny, a jego użycie i funkcja nie musi wymagać hali kilku osób;

6. Wreszcie, zważywszy na okoliczności, które nakazują jej zastosowanie, konieczne jest, aby system był łatwy w użyciu i nie wymagał ani wysiłku umysłowego, ani znajomości długiego zestawu zasad.

Nie ma korzyści, którą można uzyskać, polegając na algorytmie, który nie został poddany otwartej ocenie, szczególnie gdy istnieją silne, sprawdzone algorytmy. Uważaj na dostawców szyfrowania lub producentów dowolnych produktów zabezpieczających, którzy twierdzą, że siła jest oparta na tajnych algorytmach. Takie twierdzenia często dotyczą oleju wężowego

STEGANOGRAFIA

Zamiast szyfrowania danych za pomocą kryptografii, można również w ukryty sposób wstawiać dane do innych strumieni danych. Steganografia (dosłownie pisane po grecku) zazwyczaj wykorzystuje bity niskiego rzędu strumienia danych - zazwyczaj obraz - aby przekazać czytelny tekst. W dzisiejszych reprezentacjach obrazów kolorowych o wysokiej rozdzielczości, modyfikowanie najmniej znaczących bitów piksela powoduje znikomą zmianę koloru, przynajmniej dla ludzkiego oka. Oprogramowanie

steganograficzne może wprowadzać zmiany, a następnie wyodrębniać je ze zmodyfikowanego obrazu. Takie zmodyfikowane obrazy są trudne do zidentyfikowania, ale istnieją narzędzia wykrywające steganografię, które polegają na wykrywaniu nietypowych wzorców w pikselach obrazu nośnego. Na przykład oprogramowanie StegoHuntTM i StegoAnalyst firmy Wetstone Technologies może identyfikować i analizować dane zmodyfikowane steganograficznie; StegoBreak może wyodrębnić tekst jawny z pliku operatora