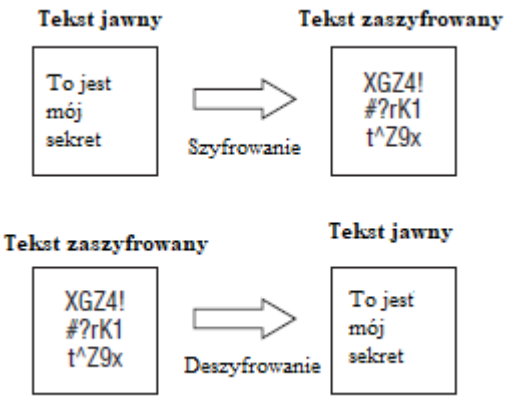
Kryptografia to badanie algorytmów szyfrowania i szyfrowania. W sensie praktycznym szyfrowanie polega na przekształceniu wiadomości z zrozumiałej formy (tekstu jawnego) w niezrozumiałą (tekst zaszyfrowany) i z powrotem. Celem szyfrowania jest uniemożliwienie odczytania danych przez przechwytywaczy lub osoby podsłuchujące, które nie znają sekretu odszyfrowywania wiadomości. Szyfrowanie ma na celu zapewnienie poufności w komunikacji. Kryptografia definiuje techniki stosowane w szyfrowaniu. W tym rozdziale omówione zostaną algorytmy szyfrowania i kryptografia.

Kryptografia i techniki szyfrowania

Szyfrowanie może służyć do szyfrowania danych podczas ich przesyłania lub podczas przechowywania na dysku twardym. Kryptografia to nauka o ochronie informacji poprzez matematyczne szyfrowanie danych, aby nie można było ich odczytać bez znajomości formuły matematycznej użytej do jej szyfrowania. Ta formuła matematyczna jest znana jako algorytm szyfrowania. Kryptografia składa się z dwóch słów: krypty (oznaczającej ukryte lub ukryte) i graficznej (oznaczającej pisanie). Kryptografia dosłownie oznacza tajne lub ukryte pisanie. Tekst jawny to czytelne i zrozumiałe dane, a tekst szyfrowany to szyfrowany tekst w wyniku procesu szyfrowania. Tekst szyfrowania powinien być nieczytelny i nie może zawierać powtarzalnego wzoru, aby zapewnić poufność danych. Rysunek 14.1 pokazuje tekst jawny a tekst zaszyfrowany.



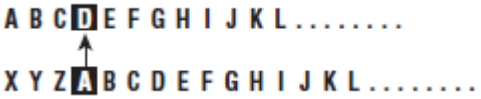
Istnieją trzy kluczowe elementy bezpieczeństwa danych. Poufność, integralność i uwierzytelnianie są znane jako triada CIA

Szyfrowanie danych zapewnia poufność, co oznacza, że dane mogą być odczytywane tylko przez upoważnionych użytkowników. Hash wiadomości zapewnia integralność, która zapewnia, że wysyłane dane są tymi samymi odebranymi danymi, a informacje nie zostały zmodyfikowane podczas przesyłania. Podpisy cyfrowe wiadomości zapewniają uwierzytelnianie (zapewniające użytkownikom to, kim są) oraz integralność. Szyfrowanie wiadomości i podpisy cyfrowe zapewniają poufność, uwierzytelnianie i integralność. Algorytmy szyfrowania mogą wykorzystywać proste metody

szyfrowania znaków, takie jak podstawianie (zastępowanie znaków innymi znakami) i transpozycja (zmiana kolejności znaków). Algorytmy szyfrowania to matematyczne obliczenia oparte na zamianie i transpozycji. Oto kilka wczesnych systemów kryptograficznych:

Szyfr Cezara Prosty szyfr zastępujący

Alfabet normalny



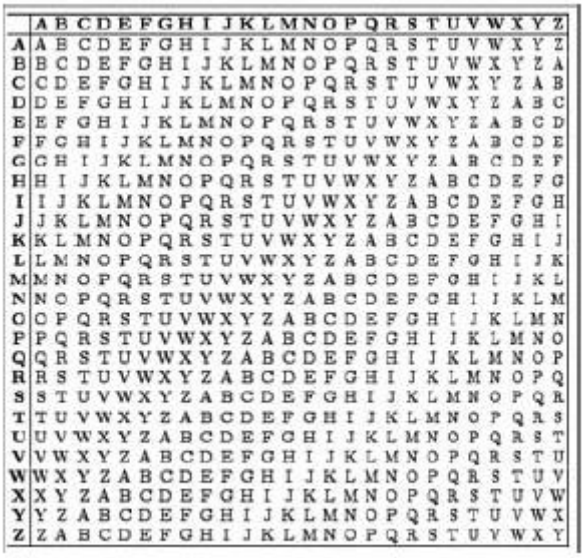
Alfabet Cezara

Szyfr Atbash Używany przez starożytnych Hebrajczyków, Atbash jest szyfrem zastępczym i działa poprzez zastąpienie każdej litery używanej z inną literą w tej samej odległości od końca alfabetu; na przykład A zostanie wysłane jako Z, a B zostanie wysłane jako Y.

Alfabet normalny

Alfabet ATBASH

Szyfr Vigenere Szesnastowieczny francuski kryptolog Blaise de Vigenere stworzył szyfr polialfabetyczny, aby przezwyciężyć niedociągnięcia prostych szyfrów zastępczych. Szyfr Vigenere używa tabeli do zwiększenia dostępnych wartości podstawienia i uczynienia podstawienia bardziej złożonym. Tabela podstawiania składa się z kolumn i wierszy oznaczonych od "A" do "Z." Aby uzyskać tekst zaszyfrowany, najpierw należy wybrać kolumnę zwykłego tekstu, a następnie wybrać wiersz klucza. Przecięcie wiersza i kolumny nazywa się tekstem szyfrowania. Aby rozszyfrować tekst szyfru, wybierz wiersz klucza i znajdź punkt przecięcia, który jest równy tekstowi szyfru; etykieta kolumny nazywa się zwykłym tekstem.



	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	W	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

Szyfr Vernama . W 1917 r. Inżynier AT & T Bell Labs Gilbert Vernam dążył do ulepszenia szyfru Vigenere i w rezultacie do stworzenia szyfru Vernam, czyli "szyfr z kluczem jednorazowym". Szyfr Vernama to algorytm szyfrowania, w którym zwykły tekst jest łączony z losowym klawiszem lub "klucz", który ma taką samą długość jak wiadomość. Szyfry z kluczem jednorazowym są jedynym algorytmem, który jest nie do złamania dzięki brute-force.

Ukryty szyfr Szyfr ukrywający tworzy komunikat, który jest w jakiś sposób ukryty. Na przykład poniższy akapit zawiera tajną wiadomość: I have been trying to buy Sally some nice jewelry, like gold or silver earrings, but prices now have increased. Kluczem jest spojrzenie na każde szóste słowo w zdaniu. Tak więc sekretna wiadomość to "buy gold now".

Rodzaje szyfrowania

Dwa podstawowe typy szyfrowania to szyfrowanie kluczem symetrycznym i asymetrycznym

Szyfrowanie kluczem symetrycznym oznacza, że zarówno nadawca, jak i odbiorca używają tego samego tajnego klucza do szyfrowania i odszyfrowywania danych. Tajny klucz, którym może być liczba, słowo lub tylko ciąg losowych liter, jest stosowany do tekstu wiadomości w celu zmiany treści w określony sposób. Może to być tak proste, jak przesunięcie każdej litery o kilka miejsc w alfabecie. Dopóki zarówno nadawca, jak i odbiorca znają tajny klucz, mogą szyfrować i odszyfrowywać wszystkie wiadomości, które używają tego klucza. Wadą szyfrowania kluczem symetrycznym jest brak bezpiecznego sposobu udostępniania klucza między wieloma systemami. Systemy używające szyfrowania kluczem symetrycznym muszą używać metody offline do przesyłania kluczy z jednego systemu do drugiego. Jest to niepraktyczne w dużym środowisku, takim jak Internet, gdzie klienci i serwery nie znajdują się w tym samym fizycznym miejscu. Siła szyfrowania kluczem symetrycznym jest szybka, szyfrowanie masowe. Słabe strony szyfrowania kluczem symetrycznym obejmują

* Dystrybucja kluczy

* Skalowalność

* Ograniczone bezpieczeństwo (tylko poufność)

* Fakt, że nie zapewnia nieodrzucania, co oznacza, że tożsamość nadawcy może zostać udowodniona

Przykłady algorytmów symetrycznych są następujące:

* DES (standard szyfrowania danych)

* 3DES

* AES (Advanced Encryption Standard)

* IDEA (międzynarodowy algorytm szyfrowania danych)

* Twofish

* RC4 (Rivest Cipher 4)

Kryptografia kluczem asymetrycznym (lub publicznym) została stworzona, aby zaradzić słabościom symetrycznego zarządzania i dystrybucją kluczy. Ale jest problem z tajnymi kluczami: w jaki sposób można je bezpiecznie wymieniać w bezpiecznej sieci, takiej jak Internet? Każdy, kto zna tajny klucz, może odszyfrować wiadomość, dlatego ważne jest, aby klucz tajny był bezpieczny. Szyfrowanie asymetryczne wykorzystuje dwa powiązane klucze znane jako para kluczy. Klucz publiczny jest dostępny dla każdego, kto może chcieć wysłać Ci zaszyfrowaną wiadomość. Drugi klucz prywatny jest

trzymany w tajemnicy, tak że tylko ty to wiesz. Wszelkie wiadomości (tekst, pliki binarne lub dokumenty) zaszyfrowane przy użyciu klucza publicznego można odszyfrować tylko za pomocą odpowiedniego klucza prywatnego. Każda wiadomość zaszyfrowana przy użyciu klucza prywatnego może zostać odszyfrowana tylko przy użyciu zgodnego klucza publicznego. Oznacza to, że nie musisz się martwić o przekazywanie kluczy publicznych przez Internet, ponieważ są one z natury dostępne dla każdego. Problem z asymetrycznym szyfrowaniem polega jednak na tym, że jest wolniejszy niż szyfrowanie symetryczne. Wymaga to znacznie większej mocy obliczeniowej zarówno do szyfrowania, jak i odszyfrowywania treści wiadomości. Relacja między dwoma kluczami w asymetrycznym szyfrowaniu klucza jest oparta na złożonych formułach matematycznych. Jedną z metod tworzenia pary kluczy jest użycie faktoryzacji liczb pierwszych. Innym jest użycie dyskretnych logarytmów. Asymetryczne systemy szyfrowania opierają się na jednostronnych funkcjach, które działają jako zapadnia. Zasadniczo szyfrowanie polega na tym, że ten sam klucz nie może odszyfrować wiadomości, które zostały zaszyfrowane. Powiązany klucz prywatny dostarcza informacji umożliwiających odszyfrowanie. Informacja o funkcji znajduje się w kluczu publicznym, podczas gdy informacje o zapadni znajdują się w kluczu prywatnym. Każdy, kto ma klucz prywatny, zna funkcję zapadni i może obliczyć klucz publiczny. Aby korzystać z szyfrowania asymetrycznego, musi istnieć metoda przesyłania kluczy publicznych. Typową techniką jest używanie cyfrowych certyfikatów X.509 (znanych również jako certyfikaty). Certyfikat jest zbiorem informacji identyfikujących użytkownika lub serwer i zawiera nazwę organizacji, nazwę organizacji, która wystawiła certyfikat, adres e-mail użytkownika, kraj i klucz publiczny. Kiedy serwer i klient wymagają bezpiecznej, zaszyfrowanej komunikacji, wysyłają zapytanie przez sieć do drugiej strony, która odsyła kopię certyfikatu. Klucz publiczny drugiej strony można wyodrębnić z certyfikatu. Certyfikat może być również używany w celu szczegółowego zidentyfikowania posiadacza. Można użyć szyfrowania asymetrycznego do :

* Szyfrowania danych

* Podpisów cyfrowych

Można zapewnić szyfrowanie asymetryczne do

* Poufności

* Uwierzytelniania

* Niezaprzeczalności

Mocne strony asymetrycznego szyfrowania klawiszy obejmują:

* Dystrybucja kluczy

* Skalowalność

* Poufność, uwierzytelnienie i nieodrzucanie

Słabością asymetrycznego szyfrowania klucza jest to, że proces jest powolny i zwykle wymaga znacznie dłuższego klucza. Jest on odpowiedni tylko dla małych ilości danych ze względu na jego powolne działanie.

Szyfr strumieniowa vs. Szyfr blokowy

Szyfry blokowe i szyfry strumieniowe to dwa typy szyfrów. Szyfrowanie blokowe to szyfry które działają poprzez szyfrowanie ustalonej kwoty lub "blok" danych. Najczęstszy rozmiar bloku to 64 bity danych. Ten fragment lub blok danych jest zaszyfrowany jako jedna jednostka tekstu jawnego. Kiedy szyfry

blokowe są używane do szyfrowania i deszyfrowania, wiadomość jest dzielona na bloki bitów. Bloki są następnie poddawane jednej lub większej liczbie następujących metod szyfrowania:

* Zmiana

* Transpozycja

* Zamieszanie

* Dyfuzja

* S-Boxy

Szyfr strumieniowy szyfruje pojedyncze bity danych jako ciągły strumień bitów danych. Szyfrowanie strumieniowe zwykle wykonuje się z większą szybkością niż szyfry blokowe i nadaje się do użycia sprzętowegp. Szyfr strumienia następnie łączy bit tekstowy z pseudolosowym strumieniem bitów szyfrowania za pomocą operacji XOR (exclusive OR). Proces XOR polega na porównywaniu zwykłego tekstu z kluczem bitowym naraz i, w oparciu o logikę XOR, tworzenie tekstu zaszyfrowanego. Jeśli zwykły tekst i tajny klucz są tym samym bitem, wynikiem jest 0; jeśli są różne, takie jak 1 i 0, wynikowy zaszyfrowany bit ma wartość 1.

Generowanie kluczy publicznych i prywatnych

Gdy klient i serwer korzystają z asymetrycznej kryptografii, tworzą własne pary kluczy dla czterech kluczy: klucz publiczny serwera, klucz prywatny serwera, klucz publiczny klienta i klucz prywatny klienta. Para kluczy systemowych ma matematyczną relację, która umożliwia szyfrowanie danych za pomocą jednego z kluczy do odszyfrowania za pomocą innego klucza. Klucze te mają matematyczną relację opartą na rozkładzie liczb pierwszych, tak że każdy klucz może zostać użyty do odszyfrowania danych zaszyfrowanych za pomocą innego klucza. Gdy klient i serwer chcą wzajemnie się uwierzytelniać i udostępniać informacje, każdy z nich wysyła własny klucz publiczny do systemu zdalnego, ale nigdy nie udostępnia kluczy prywatnych. Każda wiadomość jest szyfrowana za pomocą klucza publicznego odbiorcy. Tylko klucz prywatny odbiorcy może odszyfrować wiadomość. Serwer zaszyfruje wiadomość do klienta za pomocą klucza publicznego klienta. Jedyny klucz, który może odszyfrować wiadomość jest przechowywana przez klienta, co zapewnia poufność.

Infrastruktura klucza publicznego (PKI) jest niezbędna do tworzenia certyfikatów cyfrowych. PKI to framework, który składa się ze sprzętu; oprogramowanie; zasady, które istnieją w celu zarządzania, tworzenia, przechowywania i dystrybuowania kluczy; i certyfikaty cyfrowe. Dodatkowo kompletne rozwiązanie PKI obejmuje symetryczne algorytmy, asymetryczne algorytmy, mieszanie i uwierzytelnianie cyfrowe (zwykle certyfikaty, ale może to być również Kerberos). Jedną z głównych zalet szyfrowania klucza publicznego jest jego zdolność do ułatwiania komunikacji między stronami wcześniej nieznanymi sobie nawzajem, co jest możliwe dzięki hierarchii PKI relacji zaufania. Ważne elementy infrastruktury PKI są następujące:

* Certyfikaty cyfrowe

* Urzędy certyfikacji

* Generowanie i niszczenie certyfikatu

* Zarządzanie kluczami

Omówienie organów certyfikacji

Używanie urzędu certyfikacji (CA) do sprawdzania poprawności klienta jest podobne do udostępnienia prawa jazdy do identyfikacji. Kiedy podróżuję samolotem, muszę przedstawić ważną formę identyfikacji, aby udowodnić moją tożsamość. Bezpieczeństwo portu lotniczego będzie zazwyczaj wymagało od osoby trzeciej, takiej jak państwo, wydania identyfikatora w przypadku prawa jazdy. Pracownicy ochrony mogą zakwestionować dowód osobisty, który wykonałem w domu przy użyciu mojego aparatu cyfrowego i kolorowej drukarki. Jest również mało prawdopodobne, że przyjęliby kartę biblioteczną jako formę identyfikacji, ponieważ najprawdopodobniej nie zawiera ona wszystkich niezbędnych informacji o mnie. Stan wydający prawo jazdy jest podobny do urzędu certyfikacji: zaufana strona trzecia, która jest zaufana do sprawdzania mojej tożsamości. Sam certyfikat jest podobny do licencji kierowcy, ponieważ zawiera wszystkie informacje niezbędne do sprawdzenia mojej tożsamości. CA są klejem, który łączy razem infrastrukturę klucza publicznego. Są to zasadniczo neutralne organizacje zewnętrzne, które świadczą usługi w zakresie notyfikacji certyfikatów cyfrowych. Aby uzyskać cyfrowy certyfikat od renomowanego urzędu certyfikacji, należy zidentyfikować i udowodnić tożsamość. Cyfrowe certyfikaty są sformatowane do standardu X.509 i zawierają ustawione pola. Te pola obejmują

* Wersja

* Numer seryjny

* Identyfikator algorytmu

* Emitent

* Ważność

* Nie Przed (określona data)

* Nie Po (określona data)

* Temat

* Informacje klucza publicznego

* Algorytm klucza publicznego

* Klucz publiczny

* Identyfikator unikatowy dla emitenta (opcjonalnie)

* Niepowtarzalny identyfikator podmiotu (opcjonalnie)

* Rozszerzenia (opcjonalnie)

W ćwiczeniu 14.1 zostanie wyświetlony cyfrowy certyfikat z bezpiecznej witryny internetowej.

Ćwiczenie 14 .1

Wyświetlanie certyfikatu cyfrowego

Połącz się z każdą witryną, która wymaga logowania, np. bankiem, pocztą internetową lub witryną e-commerce. Jeśli nie masz loginu do bezpiecznej witryny internetowej, utwórz konto pocztowe Google (Gmail) na stronie www.gmail.com bezpłatnie. Jeśli tworzysz konto Gmail, musisz zmienić ustawienia, aby zawsze używać HTTPS do zabezpieczania poczty e-mail. Po zalogowaniu za pomocą protokołu SSL będzie można wyświetlić certyfikat x.509 z serwera WWW.

1. Otwórz program Internet Explorer i zaloguj się do bezpiecznej witryny.

2. Kliknij menu Strona i wybierz Właściwości lub kliknij żółtą ikonę kłódki w prawym dolnym rogu ekranu przeglądarki Internet Explorer.

3. Kliknij przycisk Certyfikaty na arkuszu właściwości strony.

4. Kliknij kartę Szczegóły, aby wyświetlić wszystkie pola certyfikatów. Kliknij każde pole, aby wyświetlić wartości.

5. Określ wystawcę certyfikatu.

6. Określ datę ważności certyfikatu.

7. Wyświetl klucz publiczny certyfikatu.

Inne zastosowania szyfrowania

Uczciwość jest jednym z elementów triady CIA i zapewnia, że informacje pozostają niezmienione i mają swoją oryginalną formę. Hash to powszechna metoda zapewniania integralności wiadomości. Hash to konwersja ciągu znaków na krótszą wartość stałej długości, która reprezentuje oryginał. Jest podobny do skróconej wersji pełnych danych. Wspólne algorytmy mieszania dla podpisów cyfrowych obejmują

* SHA-1

* MD5

* RIPEMD-160

Ćwiczenie 14. 2

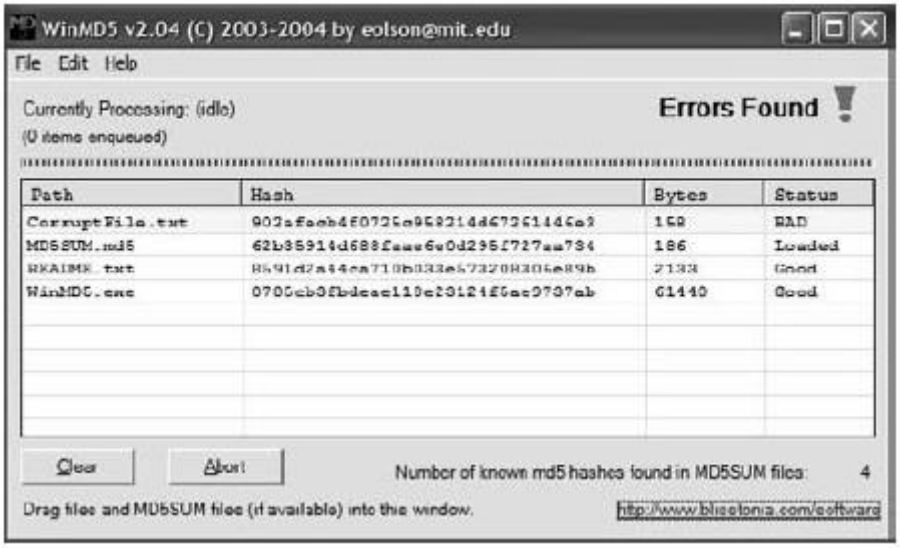
Używanie WinMD 5 do obliczania skrótów plików

1. Pobierz i zainstaluj WinMD5 ze strony www.blisstonia.com/software/WinMD5.

2. Uruchom program WinMD5.exe.

3. Kliknij menu Plik w WinMD5 i wybierz Otwórz. Wybierz dowolny plik ze swojego systemu.

Oto przykład złego skrótu MD5 dla pliku:



Jeśli pobrałeś plik z Internetu, możesz być zaniepokojony, że plik nie jest kompletny lub uszkodzony. Jednym ze sposobów zapewnienia wysyłania pliku jest ten sam otrzymany plik za pośrednictwem algorytmu mieszania MD5. Skróty MD5 to odciski palców plików. Możesz porównać odciski palców dwóch plików, aby sprawdzić, czy same pliki są takie same. Musisz mieć poprawny odcisk palca dla pliku, aby porównać otrzymany plik z oryginałem; w przeciwnym razie nie można stwierdzić, czy plik ma integralność. Gdy pobierasz duży plik, może on zawierać inny plik o nazwie MD5SUM lub coś podobnego. Ten plik zawiera prawidłowe odciski palców. Przeciągnięcie pliku MD5SUM na WinMD5 powoduje automatyczne porównanie odcisków palców. Program MD5SUM umożliwia obliczenie skrótów MD5 plików. Ułatwia również porównywanie odcisków palców z prawidłowymi odciskami palców przechowywanymi w pliku MD5SUM. Na przykład Red Hat udostępnia pliki MD5SUM dla wszystkich dużych plików do pobrania. Podczas wykonywania mieszania dwie wiadomości z tym samym skrótem są wyjątkowo mało prawdopodobne. Jeśli jednak tak się stanie, a dwa komunikaty wygenerują ten sam skrót, jest on nazywany kolizją. Kolizje umożliwiają ataki kryptograficzne na algorytm.

Algorytmy kryptograficzne

Algorytmy różnią się długością klucza od 40 bitów do 448 bitów. Im dłuższa długość klucza, tym silniejszy algorytm szyfrowania. Używanie brute-force do złamania klucza 40 bitów zajmuje od 1,4 minuty do 0,2 sekundy, w zależności od siły komputera przetwarzającego. Dla porównania klucz 64-bitowy wymaga od 50 do 37 dni na złamanie, ponownie w zależności od szybkości procesora. Obecnie dowolny klucz o długości powyżej 256 bitów jest uważany za niemożliwy do skopiowania. Message Digest 5 (MD5), Secure Hash Algorithm (SHA), RC4, RC5 i Blowfish to nazwy dla różnych algorytmów matematycznych używanych do szyfrowania. Jako etyczny haker musisz znać te algorytmy:

MD5 MD5 to algorytm mieszający, który wykorzystuje wejście o długości losowej do wygenerowania 128-bitowego skrótu. Popularnym jest tworzenie podpisu cyfrowego, który towarzyszy dokumentom i wiadomościom e-mail, aby udowodnić integralność źródła. Proces podpisu elektronicznego polega na utworzeniu skrótu wiadomości MD5 dokumentu, który jest następnie szyfrowany przez klucz prywatny nadawcy. Przetwarzanie wiadomości MD5 jest szyfrowane za pomocą klucza prywatnego w procesie podpisu cyfrowego.

SHA SHA to także skrót wiadomości, który generuje 160-bitowe szyfrowanie zaszyfrowanych danych. SHA trwa nieco dłużej niż MD5 i jest uważane za silniejsze szyfrowanie. Jest to preferowany algorytm do wykorzystania przez rząd.

* SHA-0: Wiadomość o dowolnej długości

- Wyjście: 160-bitowy odcisk palca lub skrót wiadomości

* SHA-1: Wiadomość o dowolnej długości

- Wyjście: 160-bitowy odcisk palca lub skrót wiadomości. Poprawiono błąd w oryginale algorytmu SHA-0.

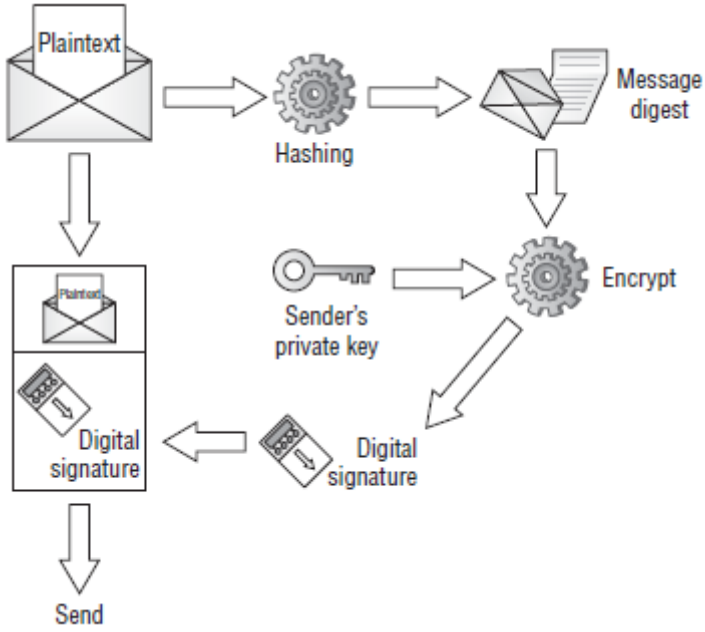
* SHA-2: Wiadomość o dowolnej długości

- Wyjście : 256-bitowy odcisk palca lub 512-bitowy odcisk palca

RC4 i RC5 RC4 jest algorytmem klucza symetrycznego i jest szyfrowaniem strumieniowym, co oznacza, że jeden bit jest zaszyfrowany w tym samym czasie. Wykorzystuje losowe permutacje matematyczne i zmienny rozmiar klucza. RC5 jest algorytmem następnej generacji: wykorzystuje zmienny rozmiar bloku i zmienny rozmiar klucza. RC5 został złamany przy rozmiarach kluczy mniejszych niż 256.

Blowfish Blowfish to 64-bitowy szyfr blokowy, co oznacza, że szyfruje dane w porcjach lub blokach. Jest silniejszy niż szyfr strumienia i ma zmienną długość klucza między 32 a 448 bitami. MAC (Message Authentication Code) MAC wymaga od nadawcy i odbiorcy udostępnienia tajnego klucza.

HMAC (Hashed Message Authentication Code) HMAC został zaprojektowany tak, aby był odporny na atak wielokolizyjny. Funkcje HMAC za pomocą algorytmu mieszającego, takiego jak MD5 lub SHA-1, i zmieniają stan początkowy za pomocą klucza symetrycznego. Nawet jeśli ktoś może przechwycić i zmodyfikować dane, jest to mało przydatne, jeśli ta osoba nie ma tajnego klucza. Nie ma łatwego sposobu na odtworzenie zakodowanej wartości bez klucza. Podpisy cyfrowe



oparte są na kryptografii klucza publicznego i służą do weryfikacji autentyczności i integralności wiadomości. Podpis cyfrowy tworzony jest przez podanie treści wiadomości za pomocą algorytmu mieszającego. Hashowana wartość jest następnie szyfrowana przy użyciu klucza prywatnego nadawcy. Po odebraniu wiadomości odbiorca odszyfrowuje zaszyfrowaną sumę, a następnie ponownie oblicza oczekiwany skrót wiadomości. Wartości powinny być zgodne, aby

* Upewnić się, że komunikat jest nieprawidłowy

* Udowodnić, że został wysłany przez stronę, którą uważał za wysłaną

* Wykazać, że tylko ta strona ma dostęp do klucza prywatnego

Ataki kryptograficzne

Ataki kryptograficzne to metody unikania zabezpieczeń systemu kryptograficznego poprzez znajdowanie słabych punktów w szyfrowaniu, protokole lub zarządzaniu kluczami. Poniżej przedstawiono ataki kryptograficzne, które mogą zostać wykonane przez atakującego:

* Atak tylko przy użyciu szyfrowania Ten atak wymaga od atakującego uzyskania kilku wiadomości zaszyfrowanych przy użyciu tego samego algorytmu szyfrowania. Kluczowymi wskaźnikami ataku tylko zaszyfrowanego są:

- Atakujący nie musi wiązać tekstu jawnego .

- Atakujący próbuje złamać kod, szukając wzorców i korzystając z analizy statystycznej.

* Atak znanym tekstem jawnym Ten atak wymaga, aby atakujący miał czysty tekst i tekst szyfrowania jednej lub więcej wiadomości. Celem jest odkrycie klucza. Ten atak może być użyty, jeśli znasz część zwykłego tekstu wiadomości.

* Atak wybranym tekstem jawnym Ten typ ataku jest przeprowadzany, gdy atakujący ma zwykłe wiadomości tekstowe wybrane przez nich zaszyfrowane. Osoba atakująca może przeanalizować wyjście szyfrowania z tekstu szyfrowania.

* Atak wybranym tekstem zaszyfrowanym. Przy użyciu tego ataku, ten rodzaj ataku jest przeprowadzany, gdy atakujący może odszyfrować fragmenty wybranej przez siebie wiadomości tekstowej szyfrowania. Atakujący może użyć odszyfrowanej części wiadomości, aby odkryć klucz.

* Atak typu "powtórka" pojawia się, gdy atakujący może przechwytywać klucze kryptograficzne i używać ich ponownie w późniejszym terminie do szyfrowania lub odszyfrowywania wiadomości, do których mogą nie mieć dostępu.

* Atak brute-force obejmuje próbowanie wszystkich możliwych kombinacji (takich jak klucze lub hasła) do momentu zidentyfikowania poprawnego rozwiązania. Ataki Brute-Force są zwykle skuteczne, ale wymagają czasu i są zazwyczaj kosztowne.

Podsumowanie

Kryptografia została stworzona w celu zachowania tajemnic przed osobami nieupoważnionymi do przeglądania informacji. Celem kryptografii jest utrzymanie tych informacji w tajemnicy, przy jednoczesnym zapewnieniu, że mogą podróżować przez niezabezpieczone sieci, takie jak Internet, niezmienione i niezmienione. W wielu przypadkach kryptografia jest po prostu sposobem na opóźnienie przeglądania informacji przez pewien czas, dopóki informacje nie będą już przydatne. Klucze tajne szyfrowania symetrycznego są używane przede wszystkim do szyfrowania danych masowych, podczas gdy klucze asymetryczne służą do bezpiecznego przesyłania tajnego klucza do systemu.

Do Zapamiętania !

* Zdefiniowałeś dwa rodzaje szyfrowania. Szyfrowanie klucz symetrycznym i szyfrowanie kluczem asymetrycznym to dwa główne typy szyfrowania.

* Zapoznałęś się z metodami wykorzystywanymi do szyfrowania danych podczas szyfrowania. Substytucja i Metody transpozycji są podstawą szyfrowania i służą do szyfrowania danych podczas procesu szyfrowania.

* Zidentyfikowałeś typowe algorytmy szyfrowania. MD5, SHA, RC4, RC5 i Blowfish które są najczęstsze algorytmy szyfrowania.

* Dowiedziałeś się, jak tworzone są klucze publiczne i prywatne. Klucz publiczny i klucz prywatny są tworzone jednocześnie jako para kluczy i służą do szyfrowania i odszyfrowywania danych. Dane zaszyfrowane za pomocą jednego elementu pary kluczy mogą być odszyfrowane tylko przez drugą.

* Poznałeś definicję kryptografii. Kryptografia to proces szyfrowania danych poprzez matematyczny proces szyfrowania danych znany jako algorytm szyfrowania.