Kryptografia-0

-zachowanie informacji dla osób wtajemniczonych

-mimo że włamujący się ma dostęp do informacji zaszyfrowanej

-mimo że włamujący się zna (?) stosowaną metodę szyfrowania

-mimo że włamujący się zna część informacji np. co do metody szyfrowania

przykład ze starożytności: około 489 r. p.n.e.

tatuaż na głowie niewolnika Histiajos → Aristagoras z Miletu

niewidzialny atrament (pisze o nim Pliniusz Starszy I wiek n.e.)

ugotowane jajko (Giovanni Porta, XVI wiek)

Kryptografia-1

-**kryptografia** - przetworzenie komunikatu w taki sposób, aby stał się nieczytelny;

-**steganografia** - ukrycie faktu istnienia komunikatu.

Gdy kanał transmisji jest znany potencjalnym włamywaczom, pozostaje tylko kryptografia.

(”nawet wiedząc że jest to wiadomość, nie potraficie jej odczytać”)

Dygresja o steganografii

steganografia właściwa (czysta) - siła techniki opiera się na nieznajomości metody przez stronę atakującą.
steganografia z kluczem prywatnym - przed rozpoczęciem komunikacji strony ustalają klucz steganograficzny wykorzystywany w sposób zależny od metody, istotny problem to przekazanie klucza w bezpieczny sposób (podsłuchujący znają metodę, ale nie znają klucza); np. metoda modyfikacji najmniej znaczącego bitu plików grafiki rastrowej czy cyfrowo zapisanego dźwięku.

Dygresja o steganografii

steganografia z kluczem publicznym i prywatnym - podobnie jak w asymetrycznych systemach kryptograficznych używane są dwa klucze - publiczny i prywatny. Klucz publiczny (jawny) wykorzystywany jest przy osadzaniu wiadomości w nośnej, natomiast klucz prywatny przy jej wyodrębnianiu. Podsłuchujący znają metodę, ale nie znają klucza prywatnego.
(np. klucz publiczny to zrobienie zdjęcia, zaś klucz prywatny to szczególny proces chemiczny w którym zdjęcie jest wywoływane i utrwalane)

Kryptografia-2

Algorytmy kryptograficzne inaczej nazywane szyframi

szyfrowanie,deszyfrowanie

Idealna sytuacja: szyfrowanie i deszyfrowanie łatwe, dane zaszyfrowane niedostępne dla osób postronnych (potencjalni włamywacze)

W szyfrowaniu jako zabezpieczenia używa się specjalnych informacji zwanych kluczem.

Kryptografia-3

Szyfrowanie ze względu na podział kluczy:

-szyfrowanie symetryczne (ten sam klucz od szyfrowania i do deszyfrowania)

-szyfrowanie asymetryczne: klucz szyfrujący (inaczej:publiczny) oraz klucz deszyfrujący (inaczej:prywatny)

Kryptografia-4

DES – (Data Encryption Standard) – najpopularniejszy szyfr symetryczny; np. podobnego używała niemiecka ENIGMA podczas II Wojny Światowej.

Blok tekstu oryginalnego szyfruje się przez wykonanie na nim ciągu permutacji i podstawień. Te permutacje i podstawienia są funkcją np. 16 podkluczy pochodzących od klucza początkowego, KP.Aby zaszyfrować blok, do danych stosuje się po kolei klucze K1,..,K16, za pomocą każdego wykonuje się pewne operacje.

Przy odszyfrowywaniu klucze są stosowane w odwrotnej kolejności.

Kryptografia-5

RSA – Rivest-Shamir-Adleman

(szyfr asymetryczny, czyli z kluczem publicznym i kluczem prywatnym)

oparty jest na własnościach liczb pierwszych, w tym na własnościach tzw. funkcji Eulera f(n)

f(n) – ile jest liczb naturalnych mniejszych od n, względnie pierwszych z n (taką funkcje wprowadzamy)

Def. Dwie liczby są względnie pierwsze, jeśli jedynym ich wspólnym dzielnikiem naturalnym jest liczba 1

Kryptografia-6

Bezpieczeństwo RSA zależy od wyboru dwóch jak największych liczb pierwszych (stosuje się liczby co najmniej 200-cyfrowe w zapisie dziesiętnym) p i q. Tworzy się n = p * q

Następnie dobiera się niedużą liczbę e (najlepiej jako liczbę pierwszą), która musi być względnie pierwsza z (p-1)(q-1).

Klucz publiczny Pu=(e,n)

Korzysta się z tego, że mnożenie jest dobrą funkcją nieodwracalną, tzn. łatwo się mnoży, ale odgadnąć z wyniku jakie jest p i q jest niesłychanie pracochłonne.Dlaczego znajomość p i q jest potrzebna do złamania szyfru?

Kryptografia-7

szyfrowanie RSA:

$$\text{blok\_zaszyfrowany} = (\text{blok\_danych})^{e} \text{ modulo } n$$

Kryptografia-8

deszyfrowanie RSA:

$$\text{blok\_danych} = (\text{blok\_zaszyfrowany})^{d} \text{ modulo } n$$

Skąd wiadomo, że takie d istnieje ?
Udało się to udowodnić przy użyciu funkcji Eulera!

$$(e * d) \text{ modulo } ((p-1)(q-1)) = 1$$

RSA

Okazuje się, że jeśli znane są p oraz q, to istnieje algorytm (rozszerzony algorytm Euklidesa do znajdowania największego wspólnego podzielnika i odwrotności modulo) przy pomocy którego można znaleźć wartość d.

Klucz prywatny Pr=(d,n)

Natomiast nawet znajomość liczb e oraz n, czyli pełnego klucza publicznego praktycznie nie pomaga ! w deszyfrowaniu

Kryptografia-10

RSA

dodatkowo dla potrzeb algorytmu RSA stosuje się bardzo wydajną unikająca tworzenia dużych liczb pośrednich metodę wyliczania wielkości

$$a^b \text{ modulo } n$$

(tzw. metoda binarnego kwadratu i mnożenia)

```
static Huge modexp(Huge a, Huge b, Huge n) {

Huge            y;

/* Wyliczamy pow(a, b) % n korzystając z metody
binarnego kwadratu i mnożenia.
  na następnej folii...   */
```

```
y = 1;


while (b != 0) {
                    if (b & 1)    y = (y * a) % n;
                    a = (a * a) % n;
                    b = b >> 1;
                   }
return y;
}  /*  koniec funkcji  */
```

oto w jaki sposób algorytm binarnego kwadratu i mnożenia działa:

1) wykorzystuje się, że

(liczba1 * liczba2) modulo n jest równe

[((liczba1) modulo n) * ((liczba2) modulo n)] modulo n

2) korzysta się z oczywistej własności, że

$$\text{liczba}^{k+m} = \text{liczba}^{k} * \text{liczba}^{m}$$

teraz wystarczy zauważyć, że w zapisie binarnym liczby jej kolejne wyższe bity oznaczają kolejne potęgi liczby 2, np. jeśli liczba b w zapisie dwójkowym ma zapis 00001101, to oznacza to

$2^3 + 2^2 + 2^0$; to naturalny sposób rozłożenia liczby b na składniki, w tym przykładzie to składniki b1, b2, b3
a^b jest liczone jako iloczyn
a^{b1} razy a^{b2} razy a^{b3} ; przy czym na każdym etapie wykonuje się dzielenie (modulo n) , aby nie powstawały zbyt duże liczby; na następnej folii jeszcze raz pokazana realizacja funkcji

```
y = 1;


while (b != 0) {
                    if (b & 1)    y = (y * a) % n;
                    a = (a * a) % n;
                    b = b >> 1;
                  }
return y;
}  /*  koniec funkcji  */
```

```
void rsa_encipher(Huge plaintext, Huge *ciphertext,
Huge e, Huge n)

{

*ciphertext = modexp(plaintext, e, n);

return;

}/*  koniec funkcji szyfrującej   */
```

```
void rsa_decipher(Huge ciphertext, Huge *plaintext,
Huge d, Huge n)

{

*plaintext = modexp(ciphertext,  d,  n);

return;

}/*  koniec funkcji deszyfrującej   */
```

jeszcze uwaga: w RSA informację szyfruje się blokami;blok niepełny musi być uzupełniony do bloku pełnego (praktycznie dotyczy to tylko ostatniego bloku)

długość bloku: nie może być dłuższa (w bitach)

niż $\log_2 n$

Kryptografia-16

http://www.cryer.co.uk/glossary/r/rsa/mathematical_guts_of_rsa_encryption.html

http://world.std.com/~franl/crypto/rsa-guts.html

napisano w roku 2001:

”If **p** and ***q*** are each 1024 bits long, the Sun will burn out before the most powerful computers presently in existence can factor your n into **p** and **q** ”

Nie zostało udowodnione, że nie ma szybkich metod faktoryzacji liczby n. Nie zostało udowodnione, że jedynym sposobem złamania RSA jest dokonanie faktoryzacji liczby n.

Kryptografia-17

$d = (x(p-1)(q-1) + 1)/e$

Aby znaleźć d, wystarczy znaleźć takie naturalne x, by powyższa wartość d była całkowita

poniżej adres strony z algorytmem Euklidesa

http://en.wikipedia.org/wiki/Extended_Euclidean_algorithm