

# Kryptografia

Marzec 2009

# Kryptografia

**dziedzina wiedzy zajmująca się zasadami, narzędziami i metodami przekształcania danych w celu ukrycia zawartych w nich informacji, zapobiegania możliwości tajnego ich modyfikowania lub eliminacji dostępu do nich osobom niepowołanym.**

# Kryptografia

ogranicza się do przekształcania informacji za pomocą jednego lub więcej „*tajnych parametrów*” (np. szyfrów) i/lub związanego z tym zarządzaniem kluczami

# Szyfrowanie

**Programy do kryptowania informacji przesyłanych między komputerami:**

- PGP (Pretty Good Privacy), indywidualnie bezpłatny**
- S/MIME (Secure/Multipurpose Internet Mail Extension) wykorzystujący certyfikat X.509**
- Lotus Notes ma własną infrastrukturę kluczy, zastosowanie tylko wewnętrzne**

# Pretty Good Privacy - PGP

**Oprogramowanie, które  
wykorzystuje, generowane  
przez właściciela,  
publiczne/prywatne klucze do  
bezpiecznej elektronicznej  
korespondencji**

# Programy szyfrujące

- Dekart Private Disk Light
- MaxCrypt
- PGp
- FineCryptHandyBits Easy Crypto Deluxe
- Cryptainer
- ABC Chaos
- Secure Task
- I inne

**do szyfrowania dowolnego  
dokumentu elektronicznego,  
przez praktycznie  
nieograniczoną liczbę osób  
można stosować jeden, ten  
sam komputerowy program  
szyfrujący**

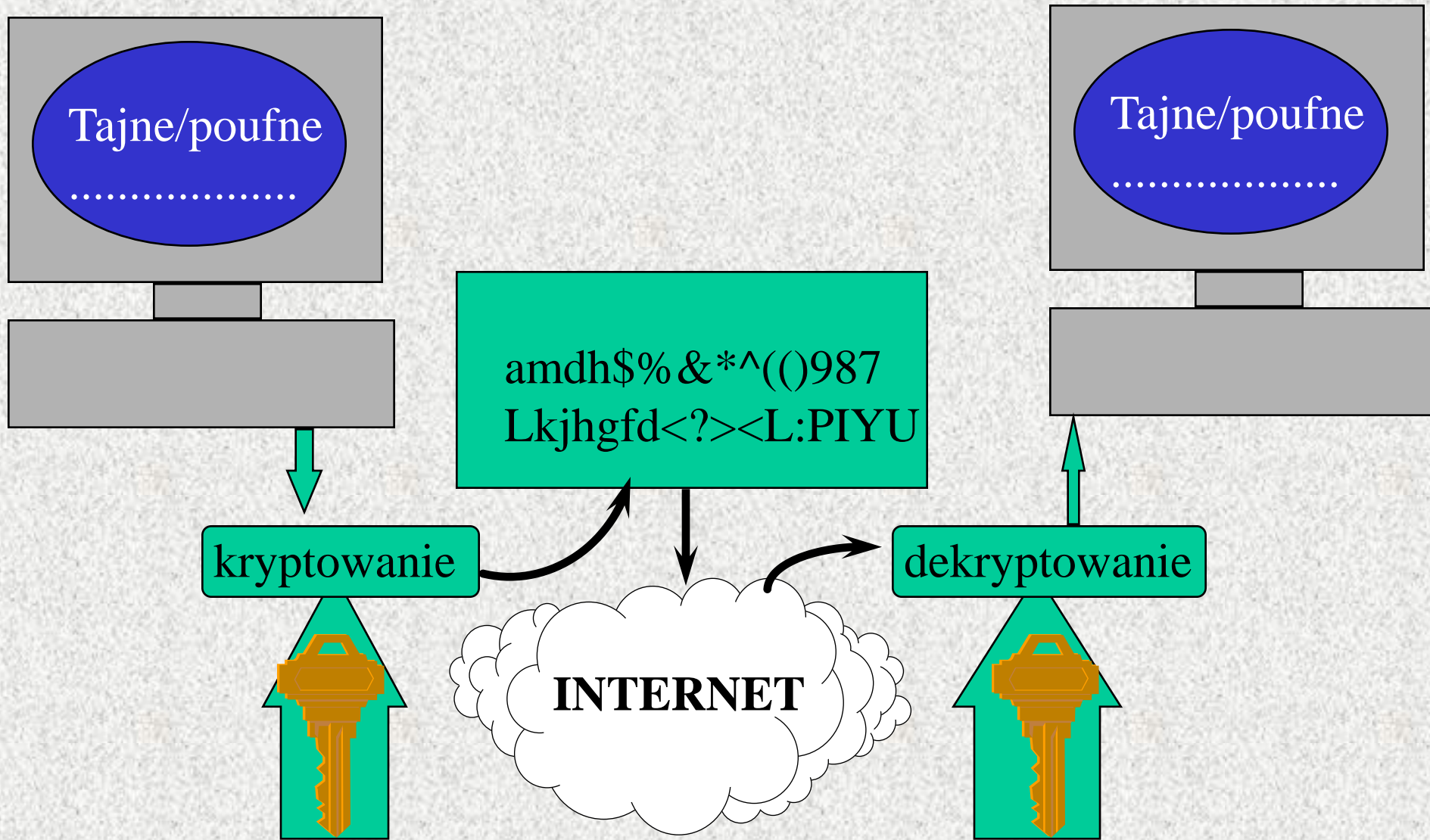


## **Klucz kodowy**

- **zazwyczaj szereg cyfr, od których zależy sposób przekształcania (szyfrowania) określonej informacji**  
**im więcej cyfr, tym bardziej skuteczny jest sposób kodowania (trudniej jest odszyfrować tak zmienioną informację)**

# Kryptografia

(symetryczny klucz)



# **Metody klucza tajnego (symetryczne)**

- **DES (Data/Digital Encryption Standard)**
- **3DES (Triple DES)**
- **RC4 (Ron's Code 4)**
- **IDEA (International Data Encryption Algorithm)**
- **Blowfish**
- **Twofish**
- **AES (Advanced Encryption Standard)**

# Zestawienie algorytmów symetrycznych

Nazwa algorytmu	Szybkość kodowania	Długość klucza	Poziom bezpieczeństwa	Uwagi
DES	średnia	56 bitów	wysoki	Standard, publiczny w USA
3DES	średnia	2x56 bitów	bardzo wysoki	Standard, publiczny w USA
IDEA	średnia	128 bitów	wysoki	Całkowicie publiczny
RC2	duża	zmienna	prawdopodobnie wysoki	Utajniony, własność RSA Inc.
RC4	bardzo duża	zmienna	prawdopodobnie wysoki	Utajniony, własność RSA Inc.

RSA

# RSA

Ideę algorytmu (RSA) szyfrowania z wykorzystaniem powiązanych ze sobą dwóch kluczy – prywatnego i publicznego opracowali w 1977 roku Ron Rivest, Adi Shamir oraz Adleman.

# Zestawienie algorytmów asymetrycznych

Nazwa algorytmu	Szybkość kodowania	Długość klucza	Poziom bezpieczeństwa	Uwagi
El Gamala	średnia	zmienna, > 512 bitów	wysoki	Podpis / szyfrowanie
RSA	bardzo duża	zmienna, > 512 bitów	wysoki / bardzo wysoki	Bardzo dużo implementacji
DSA	bardzo duża	zmienna, > 512 x 950	wysoki / bardzo wysoki	-

# Łamanie kluczy DES (56 bitów)

Liczba procesorów niezbędnych do złamania klucza

	1 rok	1 miesiąc	1 tydzień	1 dzień
1 mln/s	2300	28000	120000	830000
2 mln/s	1100	14000	60000	420000
4 mln/s	570	7000	30000	210000
32 mln/s	71	870	3700	26000
256 mln/s	9	100	470	3300

# Klucze asymetryczne

- **Publiczne/prywatne pary kluczy są niezbędne do bezpiecznej korespondencji w sieci.**
- **Publiczny klucz powinien być upowszechniony.**
- **Prywatny klucz powinien być dostępny tylko jego właścicielowi.**
- **Informacja zakodowana publicznym kluczem może być odczytana tylko przy pomocy klucza prywatnego.**



# Metody klucza publicznego (jawnego)

- **D-H (Diffie-Hellman) - uzgadnianie kluczy sesyjnych**
- **RSA (Rivest-Shamir-Adleman) - szyfrowanie i podpis**
- **ElGamala - szyfrowanie i podpis**
- **DSA/DSS (Digital Signature Algorithm/Digital Signature Standard) - podpis**
- **ECC (Elliptic Curve Cryptosystem)**

# Zagrożenia – klucz publiczny

- **Korzystaj z klucza publicznego gdy masz pewność co do jego oryginalności (otrzymałeś bezpośrednio od właściciela lub klucz jest certyfikowany)**
- **Dbaj o fizyczne bezpieczeństwo pary obu swoich kluczy**
- **Zrób kopię zapasową kluczy**

# **Zagrożenia – hasło klucza prywatnego**

- **nie stosuj słów łatwych do odgadnięcia**
- **nie stosuj pojedynczych słów**
- **użyj łatwych do zapamiętania, trudnych do odgadnięcia fraz,**

# Siła PGP

**„Gdyby zaangażować wszystkie komputery świata – 260 milionów – do rozkodowania jednej wiadomości zaszyfrowanej przy pomocy PGP, nie starczyłoby 12 milionów okresów istnienia wszechświata by tę informację odszyfrować”**

*William Crowell z NSA, 20 marca 1997 roku, za Phil Zimmermann on PGP, „Wstęp do kryptografii”, załączony do komercyjnej wersji PGP 7.1.*

# **Teoretyczne maksymalne czasy złamania kluczy klasy DES (profesjonalne)/typowe (dla np.:Netscape)**

- **40 bitów - 0,4 s/ 15 dni**
- **56 bitów - 7 godzin/ 2 691,49 lat**
- **64 bity - 74 godz. 40 min./689 021,57 lat**
- **128 bitów - 157 129 203 952 300 000 lat/  
12 710 204 652 610 000 000 000 000 lat**

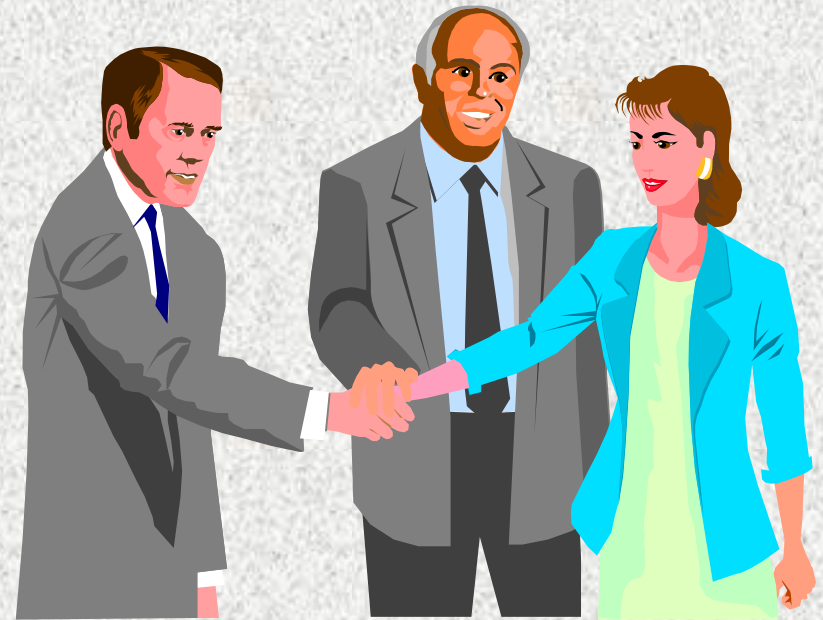
*Thom Stark, Encryption for a Small Planet, Byte, marzec 1997*

**Złamanie szyfrogramu metodą Brute-Force w jeden dzień - 256 mln operacji odszyfrowania/s**

- **56 bitów - 3 300 procesorów za 23 mln\$**
- **64 bity - 830 300 procesorów za 6 mld\$**
- **128 bitów -  $1,5 \times 10^{25}$  procesorów za  $1,1 \times 10^{29}$**

# Dystrybucja i weryfikacja kluczy

- **Kontakt bezpośredni**
- **Serwery kluczy i inne mechanizmy sieciowe**
- **CA (Certificate Authority) - instytucja poświadczająca**
- **Web of trust - sieć zaufania**



# **Trusted Third Parties**

**W niektórych krajach (pomysł USA)  
wymagane jest złożenie w TTP, przez  
użytkownika, narzędzi/kluczy  
umożliwiających, w przypadku  
sądowego dochodzenia, odczytanie  
przez odpowiednie służby,  
zaszyfrowanej przez użytkownika  
informacji**

# Secure Sockets Layer protocol **SSL**

- produkt Netscape Communications - narzędzie zapewniające prywatność i autentyczność cyfrowej komunikacji,
- nowa wersja SSL zastosowana do zabezpieczania operacji finansowych przez wiele poważnych banków
- Więcej: [http://ecommerce-guide.com/solutions/secure\\_pay/article.php/3510761](http://ecommerce-guide.com/solutions/secure_pay/article.php/3510761)

# **SSL (Secure Socket Layer)**

- **Zastąpił Secure HTTP**
- **Elastyczny - używany nie tylko z HTTP (POP3, IMAP4, SMTP, ...)**
- **Możliwa dwustronna autentykacja - certyfikaty serwera i klienta**
- **Aktualnie SSL 3.0, docelowo TLS (Transport Layer Security)**
- **stunnel - tunelowanie przez SSL**

# SSL, ale... 1/2

- połączenie realizowane przez SSL jest dobrze zabezpieczone. Gorzej jest z jego nawiązywaniem,
- ta faza, a także realizacja systemowej obsługi certyfikatów przechowywanych w Windows ma słabości,
- możliwe jest przeprowadzenie ataku typu man-in-the-middle
- użytkownik próbuje połączyć się z serwerem banku,
- działający w sieci lokalnej program zakłóca funkcjonowanie usługi DNS i przekierowuje wywołanie na adres komputera osoby atakującej.

# SSL ale... 2/2

- Tam działa aplikacja, która pośredniczy w podsłuchiwanej transmisji,
- Z jednej strony odbiera żądania klienta i przekazuje je do banku, a z drugiej odbiera odpowiedzi serwera i przesyła je do komputera ofiary.
- Połączenie pomiędzy atakowanym systemem a komputerem hakera zabezpieczone jest już podmienionym certyfikatem.
- Dlatego przeglądarka ustala parametry szyfrowania z fałszywym komputerem, a nie z serwerem banku.
- W efekcie cała transmisja przechodzi przez pośredniczący system i może być w całości odczytana przez intruza,
- Jedyne ratunek w certyfikacie, wyświetlony błąd jest zazwyczaj ignorowany, lub są inne obejścia.

# SE



## *Secure Electronic Transactions*

**Klient używa tak zwanego *portfela elektronicznego* (oprogramowanie) przechowującego numer jego karty kredytowej i publiczny, autoryzowany, klucz do jej kodowania.**



**Autoryzacja polega na wydawaniu, na każde życzenie, zaświadczenia, że dany klucz należy do osoby za którą się ona podaje**

# płatności w systemie SET

- Kupujący wysyła do e-sklepu zaszyfrowany (kluczem z e-portfela) nr karty kredytowej. 
- Sklep wysyła tak zaszyfrowany numer do banku. Tam numer jest odszyfrowany.
- Po deszyfracji, dokonany zostaje przelew na konto sklepu i przesłanie potwierdzenia wykonania tej operacji do sklepu. 
- W żadnym momencie numer karty kredytowej nie pojawia się w swojej oryginalnej postaci – zna go tylko klient i bank.

# Szyfrowanie dysków

- DriveCrypt
- Klucz upoważnia do odczytywania zawartości wirtualnego dysku.
- Dostęp: liczba dni ważności klucza, nawet godziny

# **WTLS** (ang. *Wireless Transport Layer Security*)

- służy do szyfrowania danych podczas transmisji za pośrednictwem technologii WAP.
- WTLS jest rozwiązaniem analogicznym do SSL.
- Dane są zwykle szyfrowane protokołem WTLS na drodze od klienta do bramki internetowej WAP operatora telefonii komórkowej.

# steganografia

- metoda ukrywania informacji w cyfrowych fotografiach i w plikach muzycznych.
- Steganografia nie pozostawia śladów włączania do wspomnianych plików „przemycanych” w nich informacji
- Internet w tym zakresie stanowi doskonale medium do przesyłania informacji w tej właśnie formie.

# Steganografia

- Literalnie: „ukryte pismo„
- Dane są ukryte w plikach multimedialnych
- Ukrycie = dodanie w mało znaczących bitach ukrywanej informacji – np. Ostatnie bity w zapisie pikseli obrazu.

# Przykład steganografii

- Ukrycie litery "a" (ASCII kod: 97 - 01100001) w ośmiu bitach:
  - 10010010
  - 01010011
  - 10011011
  - 11010010
  - 10001010
  - 00000010
  - 01110010
  - 00101011

# Steganografia - informacje

- Jako sposób niewidocznego podpisu fotografii, utworów muzycznych itp.
- Dobrej jakości zdjęcie (15 MB – 1600 stron)
- Darmowe programy: SecurEngine, S-Tools
- Wykrycie przez porównanie oryginału z kontenerem

# Entropia – detekcja szyfrowania

- Poziom entropii różnego rodzaju danych różni się od siebie
- Entropia może wskazać różnice zapisów (program/80, proza/95, obraz)
- Entropia może wskazać zmiany w pliku
- Entropia może pomóc w łamaniu szyfrów