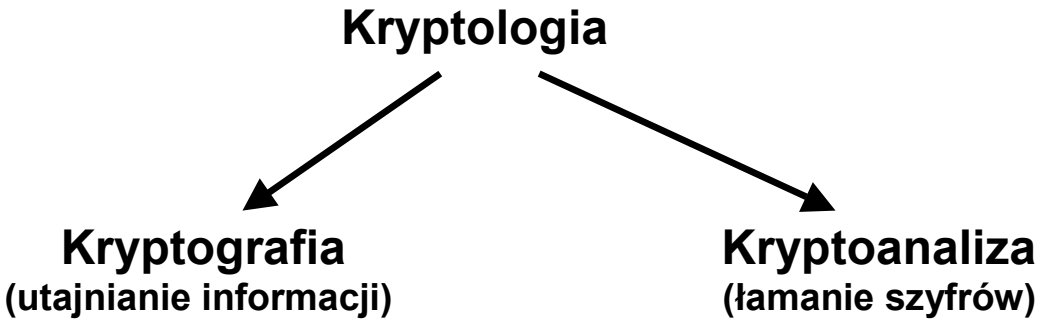


Rywalizacja kryptoanalityków i kryptografów.

Szyfrowanie – **proces, w którym wiadomość (*tekst jawny*) jest przekształcana w inną wiadomość (*kryptogram – tekst zaszyfrowany*) za pomocą funkcji matematycznej oraz hasła szyfrowania (*klucza*)**

Deszyfrowanie – **proces, w którym *kryptogram* jest przekształcany z powrotem na oryginalny *tekst jawny* za pomocą pewnej funkcji matematycznej i *klucza*.**

Zastosowanie kryptografii:

- **ochrona przed nieautoryzowanym ujawnieniem informacji przechowywanej na komputerze,**
- **ochrona informacji przesyłanej między komputerami,**
- **potwierdzanie tożsamości użytkownika,**
- **potwierdzanie tożsamości programu żądającego obsługi,**
- **uniemożliwianie nieautoryzowanej modyfikacji danych.**

Szyfrowanie jest tylko jednym z elementów strategii utrzymywania bezpieczeństwa

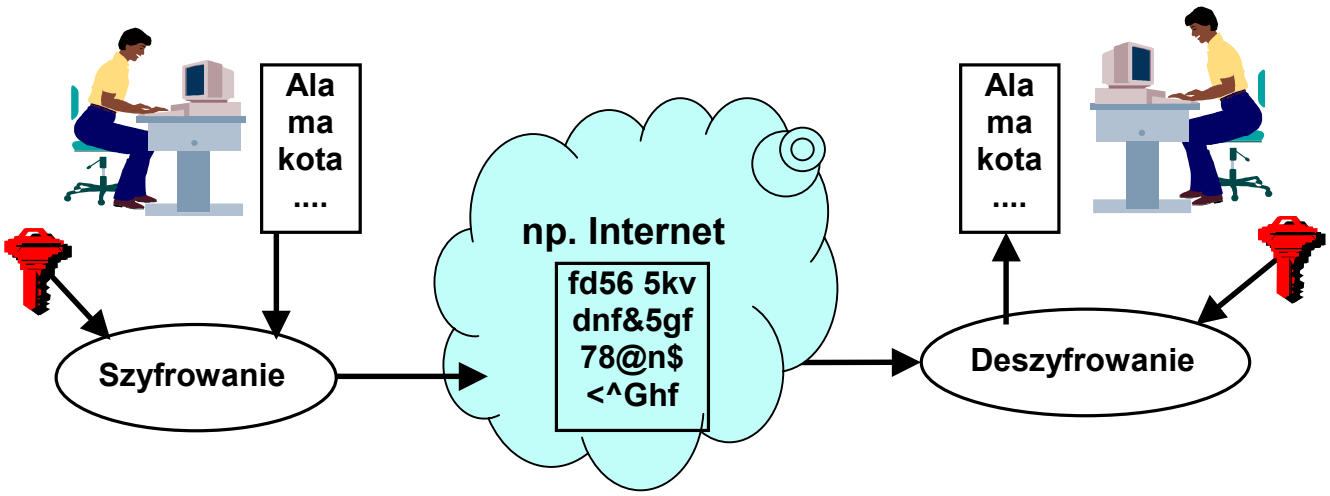
Atrybuty systemu szyfrującego

Długość klucza (w bitach)	Ilość kombinacji
40	$2^{40} \approx 1.1 * 10^{12}$
56	$2^{56} \approx 7.2 * 10^{16}$
64	$2^{64} \approx 1.8 * 10^{19}$
112	$2^{112} \approx 5.2 * 10^{33}$
128	$2^{128} \approx 3.4 * 10^{38}$

Moc kryptograficzna **– zdolność systemu kryptograficznego do ochrony danych przed atakami. Zależy od:**

- ☞ **tajności klucza**
- ☞ **trudności odgadnięcia klucza**
- ☞ **trudności *odwrócenia* algorytmu szyfrowania bez znajomości klucza**
- ☞ **istnienia sposobów odszyfrowania danych bez znajomości klucza**
- ☞ **możliwości odszyfrowania kryptogramu na podstawie znajomości części tekstu jawnego**

Szyfrowanie symetryczne

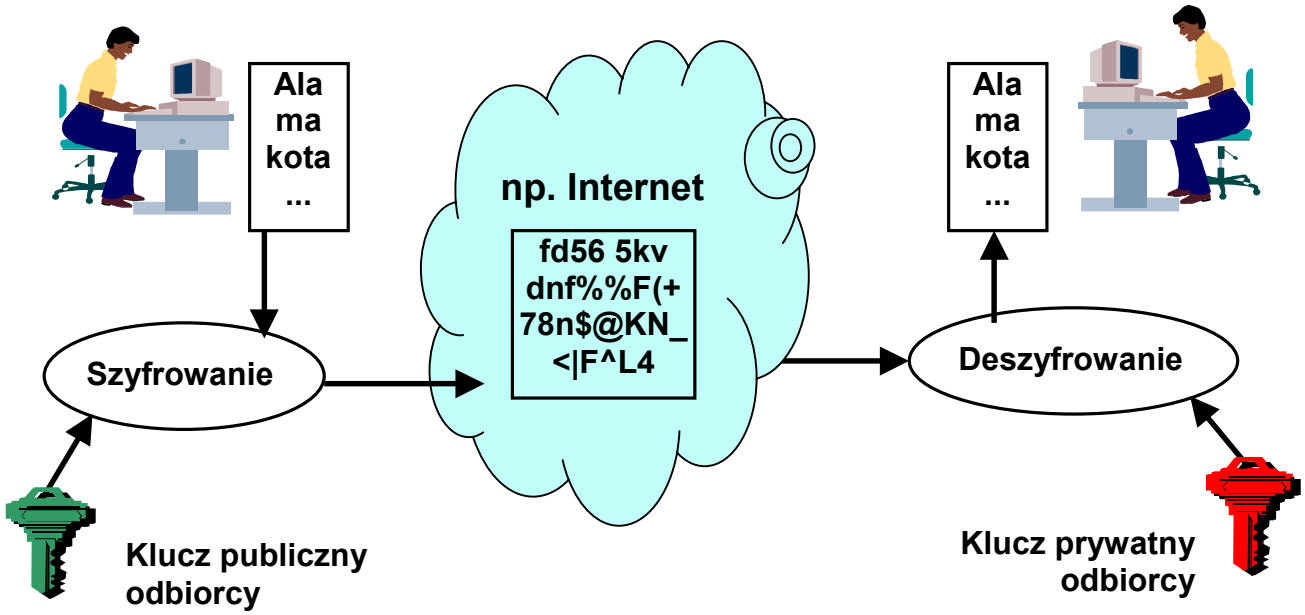


☞ **Algorytmy z kluczem prywatnym**

Szyfr Cezara	*skipjack*	*IDEA*
RC2	*RC4*	*RC5*
DES	*3DES*	

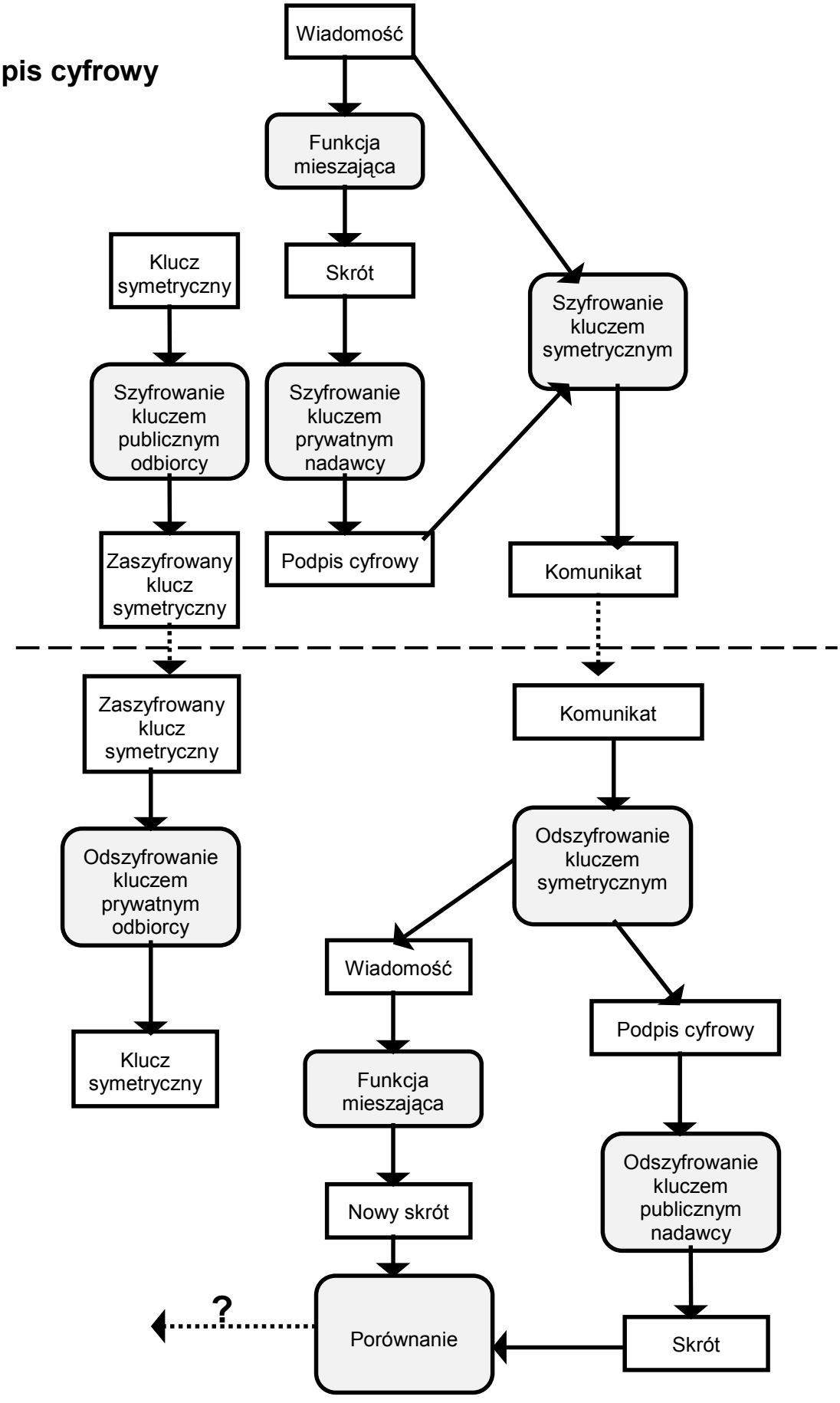
- **ECB (*Electronic Code Book*) - elektroniczna książka kodów.**
- **CBC (*Cipher Block Chaining*) - wiązanie bloków zaszyfrowanych.**
- **CFB (*Cipher FeedBack*) - szyfrowanie ze sprzężeniem zwrotnym.**
- **OFB (*Output FeedBack*) - szyfrowanie ze sprzężeniem zwrotnym wyjściowym.**

Szyfrowanie asymetryczne



- **Algorytmy z kluczem publicznym**
  - ***DSA***
  - ***ElGamal*** ***RSA***
- **Algorytmy haszujące**
  - **MD2** **MD4** **MD5**
  - **SHA** **Snefru** **Haval**

Podpis cyfrowy



Dystrybucja kluczy kryptograficznych

Protokół **CERBERA**

1. Abonent 1 kieruje zamówienie na klucz sesyjny do KDC.
2. KDC generuje losowy klucz sesyjny, szyfruje jego dwie kopie kluczami abonentów. Szyfruje kluczem Abonenta 2 informacje dotyczące tożsamości Abonenta 1:

   $$E_{A1,KDC}(K_{SES}, E_{A2,KDC}(K_{SES}, I_{A1}))$$

   i wysyła utworzony w ten sposób komunikat do Abonenta 1.
3. Abonent 1 deszyfruje swoją kopię klucza:

   $$D_{A1,KDC}(K_{SES}, E_{A2,KDC}(K_{SES}, I_{A1}))$$

4. Abonent 1 wysyła Abonentowi 2 jego kopię klucza oraz informację o swojej tożsamości:

   $$E_{A2,KDC}(K_{SES}, I_{A1}))$$

5. Abonent 2 deszyfruje swoją kopię klucza i informacje o nadawcy:

   $$D_{A2,KDC}(K_{SES}, I_{A1}))$$

6. Abonenci realizują wymianę wiadomości, gdyż każdy z nich dysponuje kluczem sesyjnym K_{SES}

Dystrybucja kluczy kryptograficznych

Protokół **SHAMIRA**

Założenie o *komutatywności* szyfru symetrycznego:

$$E_A(E_B(P)) = E_B(E_A(P))$$

1. Abonent 1 generuje klucz sesyjny do komunikacji z Abonentem 2. Szyfruje ten klucz swoim kluczem i przesyła do Abonenta 2 szyfrogram C1:

$$C_1 = E_{A1}(K_{SES})$$

2. Abonent 2 szyfruje wiadomość swoim kluczem i wysyła szyfrogram C_2 do Abonenta 1:

$$C_2 = E_{A2}(E_{A1} (K_{SES}))$$

3. Abonent 1 deszyfruje szyfrogram C_2 za pomocą swojego klucza i przesyła szyfrogram C_3 Abonentowi 2:

$$C_3 = D_{A1}(E_{A2}(E_{A1} (K_{SES}))) = D_{A1}(E_{A1} (E_{A2}(K_{SES}))) = E_{A2} (K_{SES})$$

4. Abonent 2 deszyfruje szyfrogram C_3 w celu otrzymania klucza sesyjnego:

$$D_{A2}(E_{A2}(K_{SES}))$$

5. Abonenci realizują wymianę wiadomości, gdyż każdy z nich dysponuje kluczem sesyjnym K_{SES}

Dystrybucja kluczy kryptograficznych

Protokół **WYMIANY KLUCZA ZASZYFROWANEGO**
(*EKE – Encrypted Key Exchange*)

Abonenci ustalają wspólne hasło **P**.

1. Abonent 1 generuje klucz jawny **K'** do komunikacji z Abonentem 2. Szyfruje ten klucz algorytmem symetrycznym wykorzystując klucz **P** i przesyła do Abonenta 2:

   $$E_P (K')$$

2. Abonent 2 deszyfruje wiadomość (zna hasło P), wytwarza klucz sesyjny, szyfruje go kluczem jawnym K' i kluczem tajnym P oraz wysyła szyfrogram do Abonenta 1:

   $$D_P (K') ; \qquad E_P (E_{K'} (K_{SES}))$$

3. Abonent 1 deszyfruje wiadomość i uzyskuje klucz sesyjny. Wytwarza następnie ciąg losowy $R_{A1,}$ szyfruje go kluczem sesyjnym i przesyła szyfrogram Abonentowi 2:

   $$D_P (D_{K'} (K_{SES})) ; E_{SES} (R_{A1})$$

4. Abonent 2 deszyfruje szyfrogram w celu otrzymania R_{A1}. Wytwarza następnie ciąg $R_{A2,}$ szyfruje oba ciągi kluczem sesyjnym i przesyła Abonentowi 1:

   $$D_{SES}(R_{A1}) ; \qquad E_{SES} (R_{A1}, R_{A2})$$

5. Abonent 1 deszyfruje szyfrogram w celu otrzymania R_{A1} i R_{A2} Porównuje wysłany i odebrany ciąg $R_{A1.}$ Jeżeli są zgodne, to szyfruje R_{A2} kluczem sesyjnym i przesyła Abonentowi 2:

   $$D_{SES}(R_{A1} , R_{A2}) ; \qquad E_{SES} (R_{A2})$$

6. Abonent 2 deszyfruje szyfrogram w celu otrzymania R_{A2} Porównuje wysłany i odebrany ciąg $R_{A2.}$ Jeżeli są zgodne, to oznacza, że obie strony mogą komunikować się przy pomocy klucza sesyjnego.

Dystrybucja kluczy kryptograficznych

Protokół **PODSTAWOWY** dla systemów asymetrycznych

1. Abonent 2 przesyła do Abonenta 1 swój klucz jawny:

   $$K_{JA2}$$

2. Abonent 1 generuje losowy klucz sesyjny, szyfruje go używając klucza jawnego Abonenta 2 i przesyła do Abonenta 2:

   $$E_{JA2} (K_{SES})$$

3. Abonent 2 deszyfruje wiadomość za pomocą swojego klucza tajnego (prywatnego) i uzyskuje klucz sesyjny.

   $$D_{PA2} (K_{SES}) ;$$

Dystrybucja kluczy kryptograficznych

Protokół **BLOKUJĄCY**

1. Abonent 1 przesyła swój klucz jawny Abonentowi 2:

$$K_{JA1}$$

2. Abonent 2 przesyła swój klucz jawny Abonentowi 1:

$$K_{JA2}$$

3. Abonent 1 generuje losowo klucz sesyjny, szyfruje go używając klucza jawnego Abonenta 2 i przesyła połowę zaszyfrowanej wiadomości do Abonenta 2:

$$^1/_2\ E_{JA2}\ (\ K_{SES}\ )$$

4. Abonent 2 szyfruje swoją wiadomość za pomocą klucza jawnego Abonenta 1 i też przesyła połowę wiadomości:

$$^1/_2\ E_{JA1}\ (\ K_{SES}\ )$$

5. Abonent 1 przesyła drugą połowę zaszyfrowanej wiadomości do Abonenta 2:

$$^1/_2\ E_{JA2}\ (\ K_{SES}\ )$$

6. Abonent 2 składa razem dwie połowy wiadomości i deszyfruje je, używając swego klucza prywatnego. Przesyła też drugą połowę swojej wiadomości:

$$D_{PA2}\ (\ ^1/_2\ E_{JA2}\ (\ K_{SES}\ ))\ +\ ^1/_2\ E_{JA2}\ (\ K_{SES}\ )));\qquad ^1/_2\ E_{JA1}\ (K_{SES}\ )$$

7. Abonent 1 składa razem dwie połowy wiadomości i deszyfruje je, używając swego klucza prywatnego

$$D_{PA1}\ (\ ^1/_2\ E_{JA1}\ (\ K_{SES}\ ))\ +\ ^1/_2\ E_{JA1}\ (\ K_{SES}\ )));$$

8. Abonenci realizują wymianę wiadomości, gdyż każdy z nich dysponuje kluczem sesyjnym K_{SES}

Algorytm Diffie-Hellmana

1. **Abonent 1 wybiera dużą liczbę x i oblicza $X = g^x \bmod n$**
   Abonent 2 wybiera dużą liczbę Y i oblicza $Y = g^y \bmod n$

2. **Abonent 1 wysyła liczbę X do Abonenta 2**
   (x jest utrzymywana w tajemnicy)
   Abonent 2 wysyła liczbę Y do Abonenta 1
   (y jest utrzymywana w tajemnicy)

3. **Abonent 1 oblicza: $k = Y^x \bmod n$**
   Abonent 2 oblicza: $k' = X^y \bmod n$

Czyli:

$$k = k' = g^{xy} \bmod n$$

k jest kluczem tajnym (sesyjnym)
obliczonym przez abonentów niezależnie od siebie

Literatura:

1. S.Garfinkel, G.Spafford. *Practical Unix and Internet Security.* O'Reilly & Associates 1996 (*tłum*. RM 1997).
2. V.Ahuja. *Network & Internet Security.* Academic Press 1996 (*tłum*. MIKOM 1997).
3. D.Atkins. *Internet Security: Professional Reference.* New Riders Publishing 1997 (*tłum*. LT&P 1997)
4. L.Klander. *Hacker Proof*. Jamsa Press, 1997 (*tłum.* MIKOM 1998).
5. M. Kaeo. *Designing Network Security,* CISCO PRESS 1999 (*tłum*. MIKOM 1999).
6. W. Stallings. *Network and Internetwork Security - Principles and Practice,* Prentice Hall 1994 (*tłum*. WNT 1997).