Kryptografia z kluczem publicznym

Inaczej szyfrowanie asymetryczne. Alternatywa dla szyfrowania asymerycznego. Używane do osiągnięcia poufności lub uwierzytelniania.

- Jest formą kryptosystemu, w którym szyfrowanie i deszyfracja są wykonywane za pomocą dwóch różnych kluczy – publicznego (PU) i prywatnego (PR). Inaczej nazywamy je szyfrowaniem z kluczami publicznymi.
- Tekst jawny przekształcany jest na szyfrogram przy użyciu jednego z dwóch kluczy i algorytmu szyfrującego. Deszyfracja – przy użyciu drugiego klucza i algorytmu deszyfrującego.

Klucze asymetryczne – dwa powiązane ze sobą, publiczny i prywatny, wykorzystywane do szyfrowania i deszyfracji (albo np. weryfikowania podpisu cyfrowego). Odtworzenie klucza deszyfrującego na podstawie znajomości algorytmu i klucza szyfrującego jest trudne obliczeniowo.

- *łatwe obliczeniowo* – złożoność czasowa wielomianowa (klasa złożoności *P*)
- *trudneobliczeniowo* – złożoność czasowa wykładnicza (klasa złożoności *NP*)

Różnica pomiędzy problemami P i NP: w przypadku P znalezienie rozwiązania ma mieć złożoność wielomianową, podczas gdy dla NP sprawdzeniepodanego z zewnątrz rozwiązania ma mieć taką złożoność.

Zastosowania kryptosystemów z kluczami publicznymi:

1. szyfrowanie i deszyfracja – nadawca szyfruje komunikat kluczem publicznym adresata (poufność),
2. podpis cyfrowy – nadawca podpisuje komunikat, szyfrując go swym kluczem prywatnym (uwierzytelnienie),
3. wymiana kluczy – partnerzy wymieniają klucz sesji.

	a	*b*	*c*
RSA	T	T	T
kryptografia krzywych eliptycznych	T	T	T
DSS	x	T	x
algorytm Diffiego-Hellmana	x	x	T

Próby łamania:

- *brute force* – próbowanie wszystkich możliwych kombinacji kluczy
- ataki matematyczne – próba obliczenia PR – nie są znane skuteczne metody
- *atak prawdopodobnego komunikatu* – szyfrowanie wszystkich możliwych opcji PU i porównanie z przesyłanym komunikatem

Najpopularniejszym szyfrem jest RSA, jego bezpieczeństwo wynika z trudności rozkładu dużej liczby złożonej na czynniki pierwsze. (Liczby p i q powinny być rzędu 10^{75} - 10^{100}). Próba złamania wiąże się z ogromem pracy obliczeniowej – klucz 1024-bitowy to liczba składająca się z 309 cyfr.

W 1977 roku twórcy RSA rzucili wyzwanie polegające na złamaniu szyfru. Grupie amatorów zajęło to 8 miesięcy.
Generowanie pary kluczy w systemach Unix: `ssh-keygen -t rsa`

Algorytm RSA (Rivest, Shamir, Adleman, MIT – 1977)

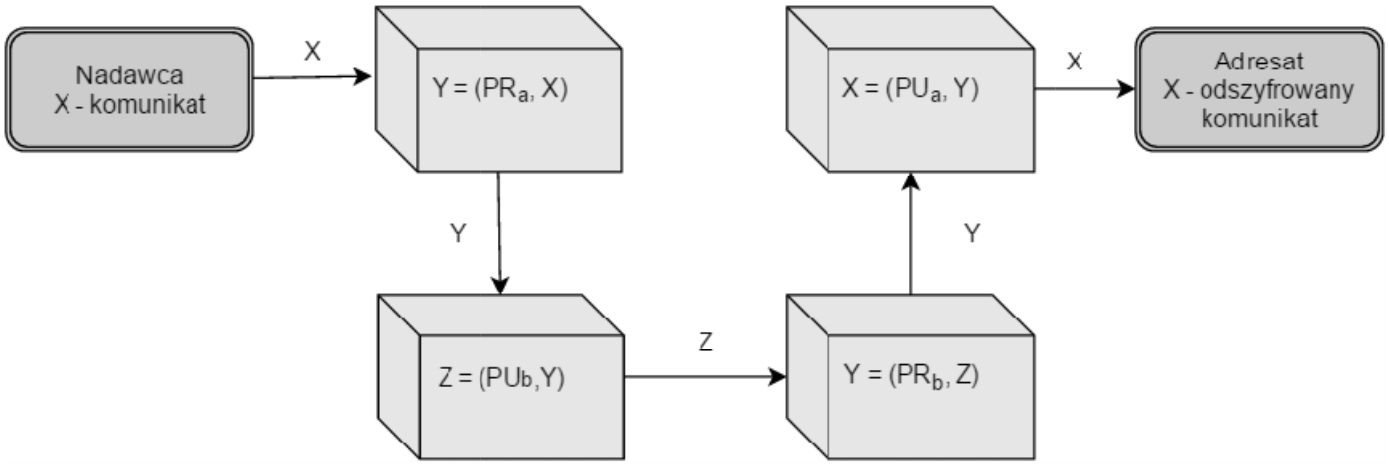
Osoba A:

1. Losuje dwie duże liczby pierwsze: $\boldsymbol{p, q}$ tż $p \neq q$
2. Oblicza wartość $\boldsymbol{n := pq}$
3. Oblicza wartość funkcji Eulera: $\mathbf{fi}(\boldsymbol{n}) := (\boldsymbol{p}-1)(\boldsymbol{q}-1)$
4. Wybiera e: $\mathbf{1 < e < fi}(\boldsymbol{n})$,
   przy czym nwd(e, fi(n)) = 1 (tzn. e i fi(n) są względnie pierwsze)
5. Znajduje liczbę d, tż $\boldsymbol{d \equiv e^{-1} (\mathrm{mod}\ \mathrm{fi}(n))}$ tzn. $d \cdot e \equiv 1$ (mod fi(n))
6. Dzieli komunikat na bloki, każdy blok szyfruje i wysyła osobie B. Przesyłane dane są postaci: $\mathbf{C := M^e \bmod n}$

Osoba B:

7. Otrzymuje zaszyfrowany komunikat **C**
8. Aby go odszyfrować, oblicza $\mathbf{M := C^d \bmod n}$

Klucz publiczny to para {e, n}, zaś prywatny – {d, n}.



Powyższy schemat gwarantuje poufność przesyłanych danych oraz uwierzytelnienie jego nadawcy. Szyfrowanie komunikatu kluczem PR pełni rolę podpisu cyfrowego – dysponując szyfrogramem Y (lecz bez znajomości PR_a) nie można zmienić tekstu jawnego X. Następnie wynik tego działania (Y) szyfrujemy kluczem PU adresata – tylko on może go odszyfrować.

Więcej informacji:

William Stallings, *Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii*, wyd. Helion, 2012