3 - RSA i El-Gamal

Tuesday, 18 June 2024 16:42

Jawna funkcja szyfrująca E

Tajna funkcja deszyfrująca D

RSA

1. Wybierzmy liczby pierwsze P, Q: $N = p \cdot q$

   $\phi(N) = (p-1)(Q-1)$

2. Niech e będzie względnie pierwsze z $\phi(N)$. ← żeby miało odwrotność!!

   Niech $d = e^{-1} \pmod{\phi(N)}$

3. $E(x) = x^e \bmod N$, $D(x) = x^d \bmod N$

Klucz publiczny: (e, N)

Klucz prywatny: d

Trudność łamania: do obliczenia ϕ potrzebujemy zfaktoryzować N.

El-Gamal

1. Ustalamy pewną grupę G (najlepiej cykliczną)

   oraz jej element g (najlepiej generator)

2. Losujemy $x \in \{1, g, \dots, g^{|G|-1}\}$

   $E = (g, g^x)$, $D = (g, x)$

Szyfrowanie wiadomości M:

1. losujemy $y \in \{1, \dots, g^{|G|-1}\}$

2. $P \to (g^y, M \cdot g^{xy})$

Trudność łamania: trudno obliczyć x mając g^x + Diffie-Hellman