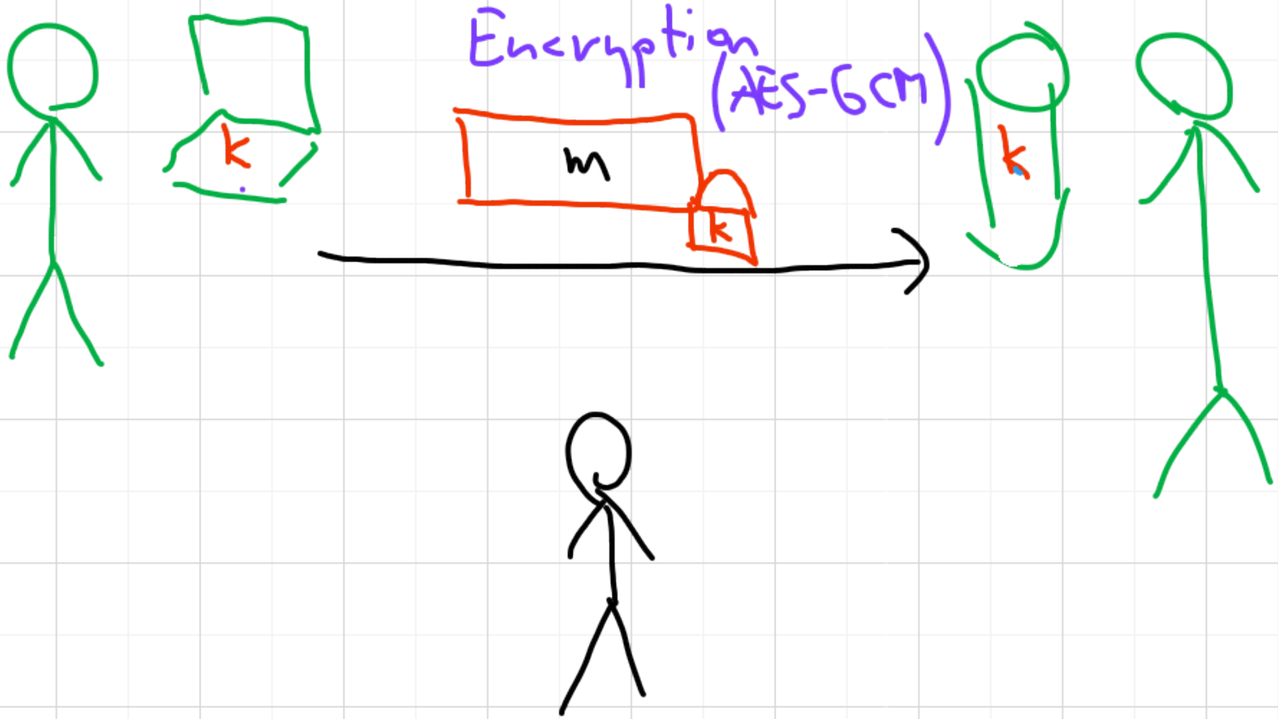
Kryptografia asymetryczna

Krypt. klucz publicznego

pubK

privK
pubK

Authenticated Encryption (AES-GCM)



k - klucz symetryczny
(do szyfrowania
i do deszyfrowania
i do uwierzytelnienia
i integralności)

Krypt asym

- szyfrowanie (pubK)
- deszyfrowanie (privK)

Podpis (privK)

Vrfy (pubK)

Key Agreement

Key Exchange

Krypt sym

- szyfrowanie (k)
- deszyfrowanie (k)

integralność

MAC k

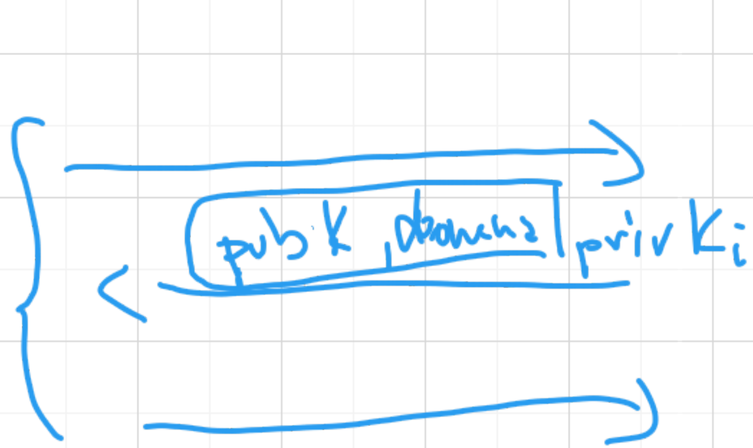
Vrfy k

pubK$_1$
pubK$_2$
⋮
pubK$_n$

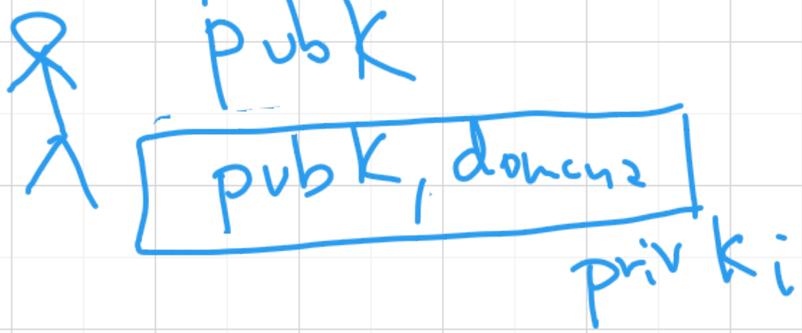
key Exchange

Diffie Hellman k

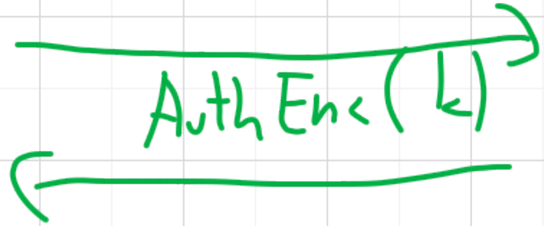
RSA sign



privK
pubK



k



RSA < alg szyfrujący
    < alg podpisów

~1977

Ronald Rivest
Adi Shamir
Michael Adelman

Atak (Faktoryzacja)

Gen(1^λ):

$p \leftarrow Prime(\lambda/2)$

$q \leftarrow Prime(\lambda/2)$

$e = 2^{16}+1$ $(e=3)$

$N = p \cdot q$

$d = e^{-1} \bmod (p-1)(q-1)$

$privK = \langle d, N \rangle$

$pubK = \langle e, N \rangle$

pubK
||
$\langle e, N \rangle$
↓
p, q

Sign(m, privK):
return $h(m)^d \bmod N$

vrfy(m, s, pubK):
return $h(m) == s^e \bmod N$

enc(m, pubK):
return $m^e \bmod N$

dec(c, privK):
return $c^d \bmod N$