

Public Key cryptography \rightarrow cryptosystems with the property that someone who knows only the

(Diffie & Hellman system 1976)

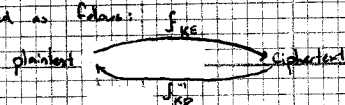
\hookrightarrow although preceded by a Cambridge mathematician working under secrecy \rightarrow James Ellis

encryption key cannot (without a prohibitively lengthy computation) discover how to decipher.

Affine cryptosystems are not public key.

Example

Could be used as follows:



K_E - enciphering key (public knowledge)

K_D - deciphering key (private)

e.g. bank communication \rightarrow want to verify

to do this, the bank chooses a secret word (pensis)

Bank encrypts this with my public key, and emails me $f_{K_E}(\text{pensis})$

Using my private key, I decrypt this, and return the word

\hookrightarrow I return the secret word, my identity is verified, as $f_{K_D}(f_{K_E}(\text{pensis}))$ only I know K_D .

RSA Public Key Cryptography

\hookrightarrow Rivest
Shamir
Adleman, 1978

- N - letter alphabet
- K - letter plaintext message units
- L - letter ciphertext message units

\rightarrow e.g. $K = 3$

MEET ME TONIGHT

\hookrightarrow MEE T-M, E-T, ONI, GHT

$L = 4$

XAYB1243

\hookrightarrow XAYB, 1243

Plaintext message units

\hookrightarrow integers in range $0 \leq i \leq N^K$

Ciphertext message units

\hookrightarrow integers in range $0 \leq i \leq N^L$

\rightarrow number of possible plaintext message units = N^K

number of possible ciphertext message units = N^L

Construction

Each user chooses two distinct random prime numbers of around 1000 digits each. (to be safe with modern technology.

\hookrightarrow choose an integer e with $\gcd(e, (p-1)) \& \gcd(e, (q-1)) = 1$

Each user computes $n = pq$ & publishes it with the enciphering key

$$K_E = (n, e)$$

Each user computes $d = e^{-1} \bmod \phi(n)$

$$(\rightarrow \phi(n) = (p-1)(q-1))$$

\hookrightarrow using the euclidean algorithm

$K_D = (n, d)$ is kept secret.

The enciphering function is $\mathbb{Z}_n \rightarrow \mathbb{Z}_n, x \mapsto x^e \bmod n$
 $f(n, e)$

$$\left[\text{Proposition: } (x^e)^d = x \bmod n \right]$$

the deciphering function is

$$f(n, d): \mathbb{Z}_n \rightarrow \mathbb{Z}_n, x \mapsto x^d \bmod n$$

MA105

Example of an RSA cryptosystem

$$N = 26 \rightarrow A = 0, \dots, Z = 25$$

$$k = 3$$

$$l = 4$$

26-letter alphabet, 2-letter p.m.u., 4-letter c.m.u.

I want to send Alice the message "YES". Her public key, found on her webpage, is $K_E^{Alice} = (46, 929, 39423)$

$$YES \leftrightarrow 24 \cdot 26^2 + 4 \cdot 26^1 + 18 \cdot 26^0 = 16,346.$$

$$f_{(n,e)}^{Alice}(YES) = 16346^{39423} \bmod 46929 = 21,166 \bmod 46,929$$

21,166 \leftrightarrow a ciphertext unit of length 4.

$$21,166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26^1 + 2 \cdot 1$$

↑
how many times does it go in?

↑
how many whole remainders?

↑
repeat

= BFIC

← ciphertext.

it is believed that the computation of d necessitates the factorisation of n into $n = p \cdot q$,

↳ this takes a prohibitive amount of time, with current technology