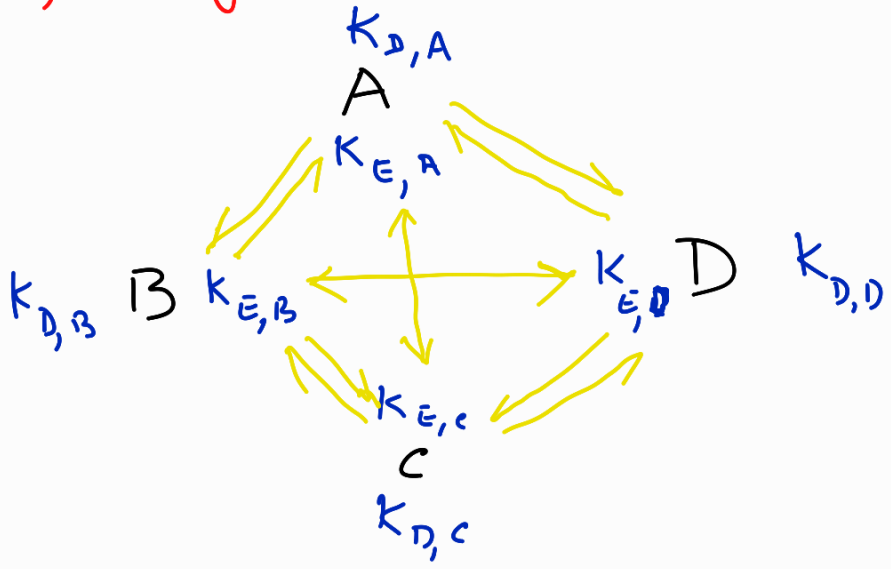
Public Key cryptography



RSA (Rivest, Shamir, Adleman).

Each user chooses two primes p and q and a random number e, which has no common factor with $\phi(n) = \phi(pq)$

$= (p-1)(q-1) = (n+1) - p - q$.

$(\because n = pq)$.

As g.c.d. $(\phi(n), e) = 1$, we can find $e^{-1} \bmod \phi(n) = d$.

Each user makes $K_E = (n, e)$ as a public key (i.e., make it public), keeping $\phi(n)$ and d as secret.

For each user $K_D = (n, d)$ is secret key.

Working modulo n, the encryption is done as follows:

$$C \equiv f(P) \equiv P^e \bmod n$$

(i.e., anyone who wants to send a plaintext message unit P to the user with public key $K_E = (n, e)$, sends $P^e \bmod n$.)

Decryption (deciphering):

$$f^{-1}(C) \equiv C^d \equiv (P^e)^d \equiv P^{ed} \equiv P \pmod n$$

[∵ Note:- if $(a, m) = 1$ and $n \equiv n' \pmod{\phi(m)}$, then $a^n \equiv a^{n'} \pmod m$]

Remark: In practice, we keep P and C uniformly throughout the system.

i.e., working in a N-letter alphabet, let $k < l$ be suitably chosen positive integers such that N^k and N^l have approximately 200 decimal digits.

We consider plaintexts to be k-graphs and ciphertexts to be l-graphs.

Each user must select p and q such that $n = pq$ and $N^k < n < N^l$.

Ex:- let $N = 26$, $k = 3$, $l = 4$. (Small numbers).

⇒ plaintexts trigraphs and ciphertexts are 4-graphs.

To send message "YES" to a user, A whose enciphering key (public key), $K_{E,A} = (n_A, e_A)$

$= (46927, 39423)$.

$YES \Rightarrow 26^2 \times 24 + 26 \times 4 + 18 = \underline{16346}$

Encryption $\Rightarrow 16346^{39423} \bmod 46927$

$\equiv 21166 \pmod{46927}$

But $21166 = 26^3 \times 1 + 26^2 \times 5 + 26 \times 8 + 2$

(∵ ciphertexts are 4-graphs).

$\Rightarrow$ "BFIC"

Decryption:- Now the reciever, with public key $K_E = (46927, 39423)$ and secret key, $K_D = (46927, 26767)$ (Deciphering key), computes as follows:

$P \equiv C^d \equiv 21166^{26767} \bmod 46927$

$\equiv 16346 = 26^2 \times 24 + 26 \times 4 + 18$

$\Rightarrow$ "YES"

Selection of Key:- The user selects $p = 281$ and $q = 167$ (secret selection).

$\Rightarrow n = 46927$

"e" is a random selection with the condition $(e, \phi(n)) = 1 \Rightarrow (e, (p-1)(q-1)) = 1$

$\Rightarrow (e, 280) = 1 = (e, 166)$.

Then computed $d = e^{-1} \bmod 280 \times 166$.

Ex:- You have recieved a trigraph message "BBI" which was encryption of a digraph plaintext in 26-letter alphabet using RSA cryptosystem. Suppose your public key is $K_E = (1073, 275)$. Read the message.

Ex:- Using RSA cryptosystem to encrypt plaintexts in digraphs to ciphertexts in trigraphy, send the message "DONE" over 26-letter alphabets, to your friend who has the public key $(n, e) = (899, 7)$. Also verify whether your friend can read the message.

Ex:- Suppose the plaintext message units are in digraphs and ciphertext message units are trigraphs. Send the message "SEND $7500" to a user A whose enciphering key is $(n_A, e_A) = (2047, 179)$. Break the code too.

Suppose 40-letter alphabet is used with numerical equivalents 0-25 for A-Z, blank = 26, ! = 27, ? = 28, $ = 29, the numerals 0-9 with numerical equivalents 30-39.

Ans:- $2047 = 23 \times 89$. $\Rightarrow \phi(2047) = 22 \times 88 = 1936$.

$e = 179$.

$d = 179^{-1} = 411 \pmod{1936}$.

$C \equiv P^e \pmod{n} \equiv P^{179} \pmod{2047}$

$\Rightarrow$ ciphertext: "BH A 2AUCAJEARO"

Discrete log:-

Discrete logarithm of y to the base b modulo "p" (a prime) is an integer x such that $b^x = y \pmod{p}$.

The Diffie-Hellman key exchange system:-

It is computationally infeasible to compute g^{ab} knowing only g^a and g^b.

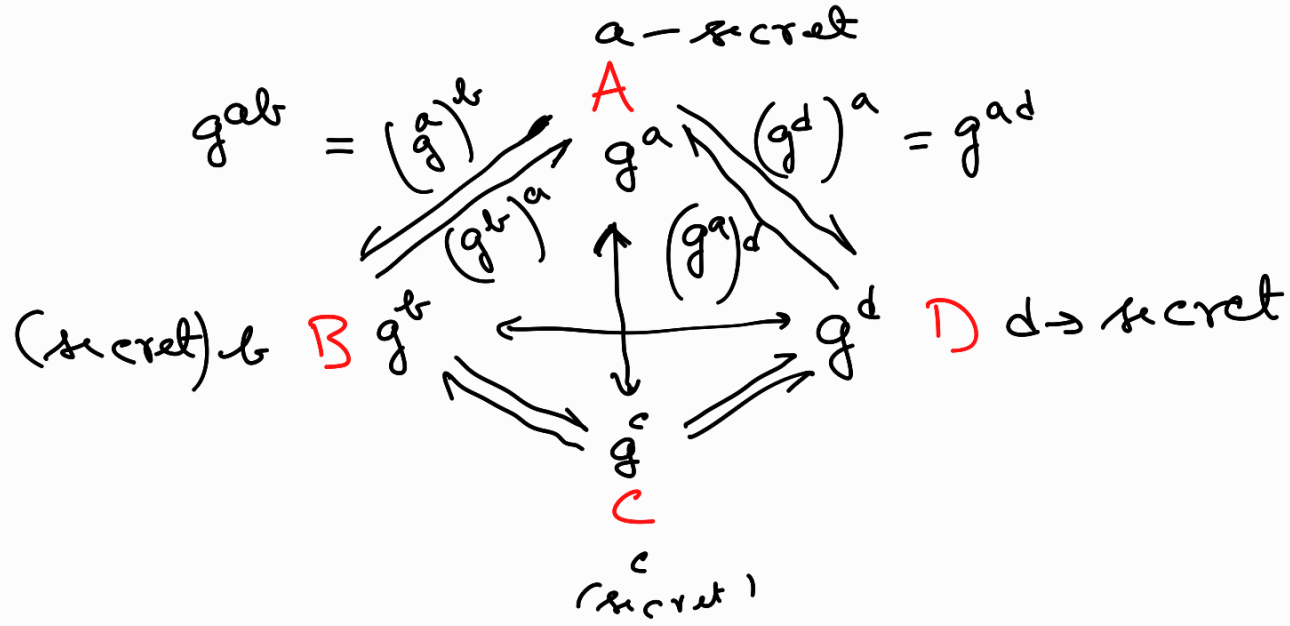
Two users A and B exchange their common key $K = g^{ab}$ in regular intervals.

A selects secret integer a and B selects secret integer b.

A and B make g^a and g^b public (keeping a and b secret) respectively.

Now A computes the common key $K = g^{ab}$ as $K = (g^b)^a = g^{ab}$.

B computes $K = (g^a)^b = g^{ab}$.



Ex:- Consider shift encryption.

$$C \equiv P + k \pmod{26}$$

Let us work in mod 53.

Let $g = 2$ (generator mod 53).

Suppose A picks $a = 29$. $\Rightarrow g^a = 2^{29} = 45 \pmod{53}$

B picks $b = 19 \Rightarrow g^b = 2^{19} = 12 \pmod{53}$

$g^a = 45$ is made public by A

$g^b = 12$ is made public by B.

Now $K = g^{ab} = (g^b)^a = 12^{29} \equiv 21 \pmod{53}$

(Computed by A)

Also, $K = (g^a)^b = (45)^{29} \equiv 21 \pmod{53}$.

$\therefore K = 21$ for both A and B

$\therefore$ Encryption: $C \equiv P + 21 \pmod{26}$

Ex:- You and your friend agree to communicate using affine enciphering transformations $C \equiv AP + B \bmod N$. Your message units are single letters in 31-letter alphabet with A-Z corresponding to 0-25, blank = 26, . = 27, ? = 28, ! = 29, , = 30. You regard key $K_E = (A, B)$ as an element $A + Bi$ (where $i^2 = -1$).

You also agree to exchange keys using the Diffie-Hellman system, and to choose $g = 4 + i$. Then you randomly choose a secret integer $a = 209$. Your friend sends you $g^b = 1 + 19i$. Read the message "BUVCFIWOUJTZ!H".

Ans:- $A + Bi = (g^b)^a = (1 + 19i)^{209} = 26 + 28i$

$\Rightarrow P \equiv 6C + 18 \pmod{31}$

$\Rightarrow$ "YOU'RE JOKING!"

$P \equiv a^{-1}c - a^{-1}b$