RSA

→ 'RSA' Crypto system (from last name of inventors Rivest, Shamir & Adleman) which is one of the oldest (16 year old) public key cryptosystems, based on difficulty of factoring

→ We now describe how RSA works:-
Each user 1st chooses 2 extremely large prime numbers p and q and sets $n = pq$
Knowing the factorisation of n, its easy to compute $\psi(n) = (p-1)(q-1)$
$= n+1-p-q$.

** → User randomly ~~chooses~~ chooses an integer e b/w 1 and $\psi(n)$ which is prime to $\psi(n)$

→ Each user A chooses 2 primes → p_A, q_A
Random number → e_A
which has no common factor with $(p_A-1)(q_A-1)$.
next

→ next A computes $n_A = p_A q_A$,
$\psi n_A = n_A + 1 - p_A - q_A$

→ e_A modulo $\psi(n_A)$, multiplicative inverse of this
Eqn is,
$\therefore d_A = e_A^{-1} \bmod \psi(n_A)$

→ She makes public the enciphering key,
$K_{E,A} = (n_A, e_A)$
and conceals the deciphering key, $K_{(D,A)} = (n_A, d_A)$

→ The Enciphering transformation is Given by:

$$f(P) = P^{e_A} \bmod n_A$$

→ deciphering transformation is Given by

$$f^{-1}(C) = C^{d_A} \bmod n_A$$

Performing f followed by f^{-1} or f^{-1} followed by f means raising to $d_A e_A{}^{th}$ power

Ex → We have → $N = 26$ $t = 3$ $\ell = 4$

i.e., plaintext consisting trigraphs
ciphertext consisting four-graphs.
in usual 26-letter alphabet.

→ To send Message → 'YES' to a user with enciphering key $(n_A, e_A) = (46927, 39423)$

→ 1st We find numerical Equivalent →

$$YES = 24 \times (26)^2 + 4 \cdot (26)^1 + 18 \times (26)^0$$
$$= 16346$$

We know,

$$f(P) = P^{e_A} \bmod n_A$$
$$= (16346)^{39423} \bmod 46927$$
$$= 21166$$

→ $21166 = 1 \times (26)^3 + 5(26)^2 + 8(26) + 2$

$= \text{"BFIC"}$

the recipient A knows the deciphering key ~~(nA, dA)~~ $(n_A, d_A) = (46927, 26767)$,

~~so computes~~ so, $f^{-1}(C) = C^{d_A} \bmod n_A$

$= (21166)^{26767} \bmod 46927$

$= 16346 = \text{"YES"}$

→ how did user A generate her keys?

1st she multiplied primes $p_A = 281$ & $q_A = 167$ to get n_A, then chooses e_A at random

then she found $d_A = e_A^{-1} \bmod 280 \cdot 166$

numbers p_A, q_A, d_A remain secret.

discrete log

one way fun^{n} →

$5^{x} \bmod 17$ → Easy

↓

from 1 to 16 ⟶ give different result for every x

→ $5^{x} \bmod 17 = 12$ → hard

↓ ↓ Given

to find

x can be 9, 25, 41, 57, 73, ---

if P is large then its hard to find 'x'

Discrete log

→ If G is a finite group, b is an element in G and y is an element of G which is a power of b then discrete logarithm of y to the base b is any integer x such that $b^x = y$.

Diffie-hellman key exchange system:-

→ In particular, process of aggreeing on a key for classical cryptosystem can be accomplished fairly efficiently using a public key system.

First proposel for doing this was based on discrete logarithmic problem.

→ Ex: Suppose we want to use an affine matrix transformation of pairs of diagraphs

$$C \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} P + \begin{pmatrix} e \\ f \end{pmatrix} \bmod N^2$$

where $0 \leq a, b, c, d, e, f < N^2$

→ P is column vector consist of numerical Equi. of 2 plaintext diagraphs.

→ taking k randomly selected integer k b/w 0 and N^2, we can take a, b, c, d, e, f to be 6 digit in k written to base N^2.

→ Now describe Diffie-Hellman method for generating a random element of large finite field F_q.

→ Suppose q is public knowledge: everyone knows what finite field our key will be in.

→ Suppose g is some fixed element of F_q, which is also not kept secret.

→ Suppose that 2 users A and B want to agree upon a key. - a random element of F_q^*. - which they will use to encrypt their subsequent message to one another.

→ A chooses an random integer a b/w 1 & $q-1$. which she kept secret.
computes $g^a \in F_q$, → Public
→ secret

→ Similarly B choose b and
g^b → public

→ Secret key they use is then g^{ab}.

Ex→ A know g^b (Public knowledge) and A also know her key a secret a. so she can compute g^{ab} but a third party only know g^a & g^b.

Ex → Suppose we are using a shift & encryption of single-letter message unit in 26-letter alphabet,

$C = P + B \bmod 26$.

→ Let $g = 2$. Let, $a = 29$, $b = 19$

Suppose A choosed $a = 29$ and

B has public → $2^b = 12$

then A can compute as $(2^b)^a = (12)^{29} = 21$ (Ans)

i.e., $B = 21$

Meanwhile for A → $2^{29} = 45$ is public,

then B can compute as $(2^a)^b$

$(45)^{19}$

→ this Example illustrates mechanics of Diffie Hellman key exchange system.