The Massey-Omura Cryptosystem for message transmission

* We suppose that everyone has agreed upon a finite field F_q, which is fixed and publicly known.

* Each user of the system secretly selects a random integer e between 0 to q-1 such that gcd(e, q-1)=1 and using the euclidian algorithm. Compute the inverse $d = e^{-1} \bmod q-1$.

* ↳ $de \equiv 1 \bmod q-1$

* If user A (Alice) wants to send a message P to Bob, first she sends him the element P^{e_A}.

* This means nothing to Bob, who not knowing d_A (or e_A) cannot recover P.

But without attempting to make sense of it, he raises it to his e_B. And sends $P^{e_A e_B}$ back to Alice.

The Third step is for Alice to unravel the message part of the way by raising to the d_A-th power: because $P^{d_A e_A} = P$. This means that she returns P^{e_B} to bob, who can read the message by raising this to the d_B^{th} power.

*NOTE

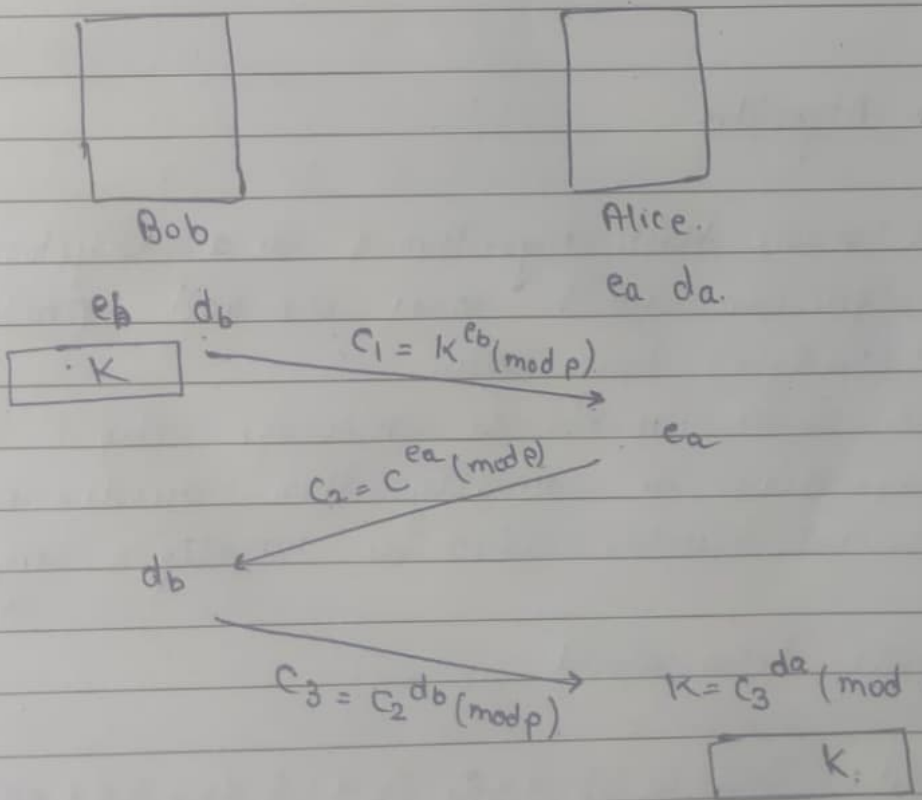
(1) It is necessary to use a good signature scheme along with the Massey-Omura system. Otherwise any person C who is not supposed to know the message P. Could pretend to be Bob, returning to Alice $P^{e_A e_C}$, not knowing that an intruder was using his own e_C. She would proceed to raise to the d_A and make it possible for C to read the message.

Thus, the message $P^{e_A e_B}$ from Bob to Alice must be accompanied by some authentication, i.e some message in some signature scheme which only Bob could have sent.

(11) It is also important that, after a user such as B or C has deciphered various messages P, and so knows various pairs (P, P^{e_A}), she cannot use that inf^n to determine e_A. i.e

Suppose Bob could solve the discrete log problem in F_q^*, thereby determining from P and P^{e_A} what e_A must be.

In that case he could quickly compute $d_A = e_A^{-1} \bmod q-1$ and then intercept and read all future messages from Alice, whether intended for him or not.



Digital Signature Standard (DSS):-

As we have seen previously, signature is very important as it is a way of authenticating the data coming from a trusted individual.

Similarly, digital signature is a way of authenticating a digital data coming from a trusted source.

* DSS is a federal information processing standard (FIPS) which defines algorithms that are used to generate digital signatures with the help of secure hash algorithm for the authentication of electronic document.
* DSS only provides us with the digital signature fn and not with any encryption or key exchanging strategies.

Secure hash Algorithm:-

SHA-1 or secure Hash Algorithm 1 is a cryptographic hash function which takes i/p and produces a 160-bit (20-byte) hash value.

This hash value is known as message digest. The message digest is usually then rendered as a hexadecimal number which is 40 digits long.

Ex. Input: hello world.

Output: 2aae6c35c94fcfb415dbe95f408b9ce91ee846ed.

Now Continuing to DSS :-

Sender side :-

In DSS Approach, a hash code is generated out of the message and following i/p are given to the signature function :-

(i) the hash code.
(ii) the random number K generated for a particular signature.
(iii) The private key of the sender i.e PR(a).
(iv) The global public key (which is a set of parameters for the communicating principles).

There i/p to the fn which provide us with the o/p signature containing two components - 's' and 'r'. Therefore, the original message concatenated with the signature is sent to the receiver.

Receiver Side :-

At the receiver end, verification of the sender is done. The hash code of the sent message is generated. There is a verification function which takes the following inputs :-

1.) The hash code generated by the receiver.
2.) Signature components 's' and 'r'.
3.) Public key of the sender.
4.) Global public key.

The o/p of the verification fn is compared with the signature component 'r'. Both the values will match if the sent signature is valid because only the sender with the help of it private key can generate a valid signature.

Pohling Hellman Algorithm

This Algorithm is used to calculate discrete Logs. This works when $p-1$ has only small factors.
Here we find the value of x:

$$\boxed{\beta = \alpha^x} \qquad 0 \le x < p-1$$

Ex: Find x such that

$$12 \equiv 7^x \bmod 41$$

Soln:

$p = 41$, $\beta = 12$, $\alpha = 7$

Now $p-1 = 40$

2	40
2	20
2	10
5	5
	1

$40 = 2^3 \times 5$

It has small factors

Therefore Pohling Hellman applicab

Let $g_1 = 2$

$g_2 = 5$

Now we will find the value of x for each g

For $g = 2$

$$x = 2^0 x_0 + 2^1 x_1 + 2^2 x_2$$

{ if there was 2^2 then $x = 2^0 x_0 + 2^1 x_1$ }

For x_0 :

$$\beta^{\frac{p-1}{g_1}} = \alpha^{\left(\frac{p-1}{g_1}\right) x_0}$$

$$12^{\frac{40}{2}} = \left(7^{\frac{40}{2}}\right)^{x_0}$$ { Fermat's Little theorem }

$$= -1 \bmod 41 = (-1)^{x_0} \bmod 41$$

Now try to put values for x_0

$x_0 = 0$: $(-1) \bmod 41 \neq (-1)^0 \bmod 41$

$x_0 = 1$: $(-1) \bmod 41 = (-1)^1 \bmod 41$

Hence $x_0 = 1$

For x_1 : First calculate β_1

$$\beta_1 = \beta \alpha^{-x_0} = 12(7)^{-1} = 31 \bmod 41$$

$$\beta_1^{\frac{p-1}{g_1^2}} = \alpha^{\left(\frac{p-1}{g_1}\right)x_1}$$

$$31^{\frac{40}{4}} = 7^{\left(\frac{40}{2}\right)x_1}$$

$$31^{10} = (7^{20})^{x_1}$$

For $x_1 = 0$, equation satisfied

Hence $\boxed{x_1 = 0}$

For x_2 : First calculate β_2

$$\beta_2 = \beta_1 \alpha^{-x_1} = 31(7)^{-0} = 31 \bmod 41$$

$$\beta_2^{\frac{p-1}{g_1^3}} = \left(\alpha^{\frac{p-1}{g_1}}\right)^{x_2}$$

$$31^{\frac{40}{8}} = \left(7^{\frac{40}{2}}\right)^{x_2}$$

$$-1 \bmod 41 = (-1)^{x_2} \bmod 41$$

$$\boxed{x_2 = 1}$$

Recall: $x = 2^0 x_0 + 2^1 x_1 + 2^2 x_2$

$= 1 \times 1 + 2 \times 0 + 4 \times 1 = 5$

$$\boxed{x = 5 \bmod 8}$$

Now we find another x from the other

$g_2 = 5$

$g_2 = 5$

$x = 5^0 x_0$

For x_0: $\beta^{\frac{p-1}{g_2}} = (\alpha^{\frac{p-1}{g_2}})^{x_0}$

$12^{\frac{40}{5}} = (7^{\frac{40}{5}})^{x_0}$

$12^8 = (7^8)^{x_0}$

$18 \equiv 37^{x_0} \bmod 41$

$x_0 = 0$, $18 \not\equiv 37^0 \bmod 41$ ✗

$x_0 = 1$, $18 \not\equiv 37^1 \bmod 41$ ✗

$x_0 = 2$, $18 \not\equiv 37^2 \bmod 41$ ✗

$x_0 = 3$, $18 \equiv 37^3 \bmod 41$ ✓

Hence $x_0 = 3$

$x = 5^0 x_0 = 1 \times 3 = 3$

$$\boxed{x = 3 \bmod 5}$$

So, $x = 5 \bmod 8$

$x = 3 \bmod 5$

From chinese remainder theorem,

$x = 13 \bmod 40$

↙

since exponents are (mod $p-1$)

Hence $\boxed{12 = 7^{13} \bmod 41}$ Ans.