

17-th of May course works should be sent to me.
 19-th of May the defendance of course works.

Bit commitment

1. Protocol based on h-functions.

2. Massey-Omura 3-pass Protocol https://en.wikipedia.org/wiki/Three-pass_protocol

3-pass protocol for sending messages is a framework which allows one party to securely send a message to a second party without the need to exchange or distribute [encryption keys](#).

B : should I must sell my bitcoins ?

A : Don't hurry, I know the price for next month.

B : then tell me please,

A : I'll tell you next month, but if you want to know immediately give me 1 BTC.

B : How it is to know me that you are not cheating?

A : We can use Bit Commitment scheme,

M is a Bitcoin price next month

1. Protocol based on H-functions.

M can be of arbitrary finite length

A :

$$h = H(M)$$

H-function
SHA-256

h

A : please send me M

M

B :

Is not able to learn anything about M since it is infeasible to find M having $h = H(M)$.

B : verifies if $h \stackrel{T}{=} H(M)$

2. Massey-Omura 3-pass Protocol

Public parameter $PP = p = 264043379$; p - may be strong prime

$A: K_A = (e_A, d_A)$
secret key of A

$B: K_B = (e_B, d_B)$
secret key of B

E.g.
In the case
of ElGamal

e_A - for encryption

e_B - for encryption

d_A - for decryption

d_B - for decryption

PKA

$$e_A \cdot d_A = 1 \pmod{p-1}$$

$$e_B \cdot d_B = 1 \pmod{p-1}$$

M - message to be encrypted

Encryption-Decryption operations: $|M| < |p|$

$$\text{Enc}(e_A, M) = M^{e_A} \pmod{p} = C$$

$$\begin{aligned} \text{Dec}(d_A, C) &= C^{d_A} \pmod{p} = (M^{e_A})^{d_A} \pmod{p} \\ &= M^{e_A \cdot d_A} \pmod{p-1} \pmod{p} \\ &= M^1 \pmod{p} = M. \end{aligned}$$

According to Fermat theorem

Remark. $e_A \cdot d_A = 1 \pmod{p-1}$ if $\gcd(e_A, p-1) = 1$, then the generation of e_A, d_A is the following

1) $\gg p = \text{genstrongprime}(28)$

$p = 264043379$;

$$p = 2 \cdot q + 1 \Rightarrow p-1 = 2 \cdot q$$

2) $\gg e_A = \text{randi}(p-1)$ % if e_A is even, then

$$\gg \gcd(e_A, p-1) = 1 \quad \% \gcd(e_A, p-1) = 2$$

3) $\gg d_A = \text{mulinv}(e_A, p-1)$

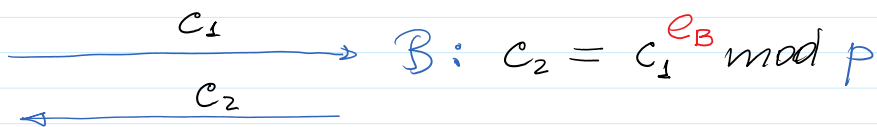
$$\gg \text{mod}(e_A * d_A, p-1) = 1$$

2. Massey-Omura 3-pass Protocol execution

A : Encrypts M with encryption function $Enc(e_A, M) = c_1$
 sends ciphertext c_1 to B . $|M| < |P|$.

$M=71\ 000$, $p = 264043379$; $\rightarrow 71\ 000 < 264043379 \rightarrow |M| < |p|$

$$E(e_A, M) = M^{e_A} \bmod p = c_1$$



After 1 month

$$A: c_3 = c_2^{d_A} \bmod p$$

$$\xrightarrow{c_3} B: c_4 = c_3^{d_B} =$$

$$= (c_2^{d_A})^{d_B} = ((c_1^{e_B})^{d_A})^{d_B} =$$

$$= (((M^{e_A})^{e_B})^{d_A})^{d_B} \bmod p =$$

$$= M^{(e_A \cdot d_A) \cdot (e_B \cdot d_B) \bmod (p-1)} \bmod p =$$

$$e_A \cdot d_A = 1 \bmod (p-1) \quad e_B \cdot d_B = 1 \bmod (p-1)$$

$$= M^{1 \cdot 1} \bmod p = M^1 \bmod p = M \bmod p$$

$$\text{If } M < p \Rightarrow M \bmod p = M = 71\ 000$$

Bit commitment: is used for auctions, public purchasing systems and etc.

```
>> p = 264043379;
>> pm1=p-1
pm1 = 264043378
>> isprime(eA)
ans = 1
>> eA=genprime(28)
```

```
>> M=71000
M = 71000
>> c1=mod_exp(M,eA,p)
c1 = 177163502
```

```
>> eB=genprime(28)
eB = 145223009
>> gcd(eB,p-1)
ans = 1
>> dB=mulinv(eB,p-1)
dB = 152146093
```

```
ans = 1
>> eA=genprime(28)
eA = 176312179
>> gcd(eA,p-1)
ans = 1
>> dA=mulinv(eA,p-1)
dA = 251630141
>> mod(eA*dA,p-1)
ans = 1
```

Dogecoin

```
M = 71000
>> c1=mod_exp(M,eA,p)
c1 = 177163502
>> c2=mod_exp(c1,eB,p)
c2 = 55675334
>> c3=mod_exp(c2,dA,p)
c3 = 6910648
>> c4=mod_exp(c3,dB,p)
c4 = 71000
```

```
ans = 1
>> dB=mulinv(eB,p-1)
dB = 152146093
>> mod(eB*dB,p-1)
ans = 1
```