`127_008_Coin-Flipping

1.Comments on MTE.
2.PR Topics.

Coin flipping, **coin tossing**, either **heads** or **tails** is the practice of throwing a coin in the air and checking which side is showing when it lands, in order to choose between two alternatives, heads or tails, sometimes used to resolve a dispute between two parties.
It is a form of sortition which inherently has two possible outcomes.
The party who calls the side that the coin lands on wins.
From <https://en.wikipedia.org/wiki/Coin_flipping>

Dice throwing

Card game - Poker

A: $PrK_A = x$, $PuK_A = a$;
b, e; $a = g^x \bmod p$

B: $PrK_B = y$, $PuK_B = b$;
a, e; $b = g^y \bmod p$;

E: $PrK_C = z$, $PuK_C = e$;
a, b; e = ---

ElGamal encryption

PP=(p, g)   **>> p = 268 435 019**; % 2^28 -1 --> >> int64(2^28-1)
% ans = **268 435 455**

>> g=2;

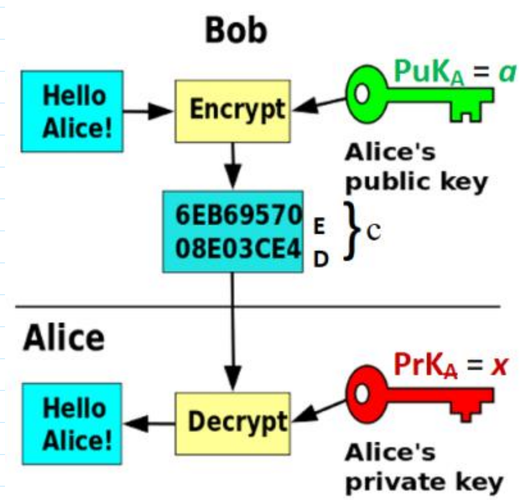
$m \in \mathbb{Z}_p^* = \{1, 2, 3, ..., p-1\}$; $*$ mod p

message to be encrypted

$i \leftarrow \text{randi}$; $i \in \mathbb{Z}_{p-1} = \{0, 1, 2, ..., p-2\}$

$c = Enc(a, i, m) =$

$$= (E, D) = (\underbrace{m a^i \bmod p}_{E}, \underbrace{g^i \bmod p}_{D})$$



$$Dec(x, c) = E \cdot D^{-x} \bmod p = \frac{E}{D^x} \bmod p =$$

$$= \frac{m a^i \bmod p}{(g^i)^x} = \frac{m (\cancel{g}^x)^i \bmod p}{\cancel{g}^{ix}} = m \bmod p = m \quad \text{if } m < p$$

D^{-x} mod ***p*** computation using Fermat theorem:
If ***p*** is prime, then for any integer ***a*** holds **a^{p-1} = 1 mod *p***.

$$D^{-x \bmod (p-1)} \textbf{ mod } p = D^{p-1-x} \textbf{ mod } p$$

D^{-x} mod p computation

a) D^{-1} computation : >> D_m1=mulinv(D, p)

b) D^{-x} computation : $(D^{-1})^x = D^{-x}$ >> D_mx=mod_exp(D_m1,x, p)

A : $PrK_A = x$; $PuK_A = a$; $PuK_B = b$;

$m_i \in \{1, 2\}$

Coin flipping scheme: ***Alice*** before coin flipping assigns possible results to variables m_1=1 and m_2=2.
1. ***Alice*** after coin flipp assigns result *m* either to *m*=1 or *m*=2.
2. ***Alice*** encrypts m_1=1 and m_2=2 by her **PuK**=***a*** using random generated numbers *i*1 and *i*2 computing ciphertexts c_{1A} and c_{2A} respectively:

$m_i \in \{1, 2\}$

$i_1, i_2 \leftarrow \text{randi}(\mathbb{Z}_{p-1})$

$$\left.\begin{array}{l} c_{1A} = Enc(a, i_1, m_1) = (E_{1A}, D_{1A}) \\ c_{2A} = Enc(a, i_2, m_2) = (E_{2A}, D_{2A}) \end{array}\right\}$$

$$E_{1A} = m_1 \cdot a^{i_1} \bmod p;\ D_{1A} = g^{i_1} \bmod p$$
$$E_{2A} = m_2 \cdot a^{i_2} \bmod p;\ D_{2A} = g^{i_2} \bmod p$$

$$\xrightarrow{C_{1A},\, C_{2A}} \quad B$$

B: $PrK_B = y$; $PuK_B = b$.

A:

$C_{2A} \leftarrow \text{rand}\{C_{1A}, C_{2A}\}$; $C_{iA} = C_{2A}$

$i_3 \leftarrow \text{randi}(\mathcal{Z}_{p-1})$

$$Enc(b, i_3, E_{2A}) = (E_{2AB}, D_{2AB}) = C_{2AB}$$
$$= \underbrace{(\underbrace{E_{2A} \cdot b^{i_3} \bmod p}_{E_{2AB}},\ \underbrace{g^{i_3} \bmod p}_{D_{2AB}})}$$

$$\xleftarrow{E_{2AB}} \quad C_{2AB}$$

$$Dec(x, C_{2AB}) = \frac{E_{2AB}}{(D_{2A})^x} = E_{2AB} \cdot (D_{2A})^{-x} =$$
$$= \frac{E_{2A} \cdot b^{i_3}}{(g^{i_2})^x} = \frac{m_2 \cdot a^{i_2} \cdot b^{i_3}}{g^{i_2 x}} =$$
$$= \frac{m_2 \cdot a^{i_2} \cdot b^{i_3}}{g^{i_2 x}} = \frac{m_2 \cdot \cancel{g^{x i_2}} \cdot b^{i_3}}{\cancel{g^{i_2 x}}} =$$
$$= m_2 \cdot b^{i_3} = E_{2ABA} \xrightarrow{E_{2ABA}} \quad B: \ C_{2ABA} = (E_{2ABA}, D_{2AB})$$

(1) Let B guessed that A tossed C_{2A}

$$Dec(y, C_{2ABA}) = E_{2ABA} \cdot (D_{2AB})^{-y} =$$
$$= \frac{E_{2ABA}}{(D_{2AB})^y} = \frac{m_2 \cdot b^{i_3}}{(g^{i_3})^y} = \frac{m_2 \cdot (g^y)^{i_3}}{g^{i_3 y}} =$$
$$= \frac{m_2 \cdot \cancel{g^{y i_3}}}{\cancel{g^{i_3 y}}} = m_2$$

$\cancel{g^{i_3 y}}$

$\xleftarrow{m_2,\ i_3}$

$m = E_{2ABA} \cdot (b)^{-i_3} \bmod p =$

$m_2 \cdot b^{i_3} \cdot b^{-i_3} = m_2 \cdot b^{i_3 - i_3} =$

$= m_2 \cdot b^0 = m_2 \cdot 1 = m_2$

$\xrightarrow{i_2}$ $\mathcal{B}$: $c_{2A} = (E_{2A}, D_{2A})$

$E_{2A} \cdot a^{-i_2} \bmod p =$

$= m_2 \cdot a^{i_2} \cdot a^{-i_2} \bmod p =$

$= m_2 \cdot a^{i_2 - i_2} = m_2 \cdot a^0 = m_2$

---

(2) Let $\mathcal{B}$ choosed that $\mathcal{A}$ tossed $c_{1A} = (m_1 \cdot a^{i_1}, g^{i_1})$

$\mathcal{B}$ did not guess the toss.

$i_3 \leftarrow \text{randi}(\mathbb{Z}_{p-1})$

$Enc(b, i_3, E_{1A}) = (E_{1AB}, D_{1AB}) = c_{1AB}$

$$= \underbrace{(\underbrace{E_{1A} \cdot b^{i_3} \bmod p}_{E_{1AB}},\ \underbrace{g^{i_3} \bmod p}_{D_{1AB}})}_{}$$

$\xleftarrow{\quad}$ c_{1AB}

$$Dec(x, c_{2AB}) = \frac{E_{1AB}}{(D_{2A})^{x}} =$$

$$= \frac{E_{1A} \cdot b^{i_3}}{(g^{i_2})^{x}} = \frac{m_1 \cdot a^{i_1} \cdot b^{i_3}}{g^{i_2 x}} =$$

$$= \frac{m_1 \cdot a^{i_1} \cdot b^{i_3}}{g^{i_2 x}} = \frac{m_1 \cdot g^{x i_1} \cdot b^{i_3}}{g^{i_2 x}} =$$

$\mathcal{B}$:

E_{1ABA}

$g^{i_2 x}$ $\qquad$ $g^{i_2 x}$

$= E_{1ABA}$ $\qquad \xrightarrow{E_{1ABA}}$ $\qquad \mathcal{B}:$

$$Dec(y, c_{1ABA}) = \frac{E_{1ABA}}{(D_{2AB})^{y}} = m'$$

$$E_{1ABA} \cdot (b)^{-i_3} \bmod p = m'' \qquad \xleftarrow{m', i_3}$$

$$\xrightarrow{m'' \ i_2} \quad \mathcal{B}: Dec(y, m'')$$

$$E_{1A} \cdot a^{-i_2} \bmod p = u \notin \{1, 2\}$$

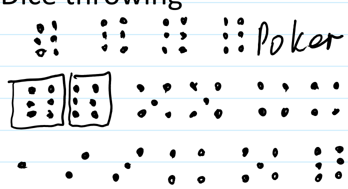
If random generated number i in ElGamal encryption is revealed then ciphertext canbe decrypted.

$$Enc(a, i, m) = (E, D) = (m \cdot a^{i} \bmod p, g^{i} \bmod p) = c$$

Decryption without knowledge $PrK = x$ but having i:

$$E \cdot a^{-i} \bmod p = m \cancel{a^{i}} \cancel{a^{-i}} \bmod p = m \bmod p = m.$$

Dice throwing



Poker

3×2

$\rightarrow \equiv 21$

$m \in \{1, 2, 3, 4, 5, 6, \ldots$

$r_1 \leftarrow randi, \ ---, \ r_6 \leftarrow randi$

$c_i = Enc(a, r_i, m_i), \ i =$ 1, 2, 3, ...

$c_1 \equiv 1; \ c_2 \equiv 2; \ c_3 \equiv 3; \ldots c_6 = \ldots \longrightarrow$ $\mathcal{B}: c_i \leftarrow rand\{c_i\}$

$\longrightarrow \quad \mathcal{C}: c_i = c_6$

$c_{ij} = Enc(a, r_{ij}, m_{ij}) \qquad c_{ij} \leftarrow rand\{c_{ij}\}$

$i =$ 1, 2, 3, ... kauliuko reikšmės

$j = \overline{1, 6}$ kauliuko numeris

Card game - Poker

52 kortos & 4 mastis

1 kortos šifrav.

$c_i = Enc(a, r_i, m_i)$; $i = \overline{1,4}$.

$c_{ij} = Enc(a, r_{ij}, m_{ij})$; $j = \overline{1,52}$.