Coin flipping, **coin tossing**, or **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

$\mathcal{A}: PrK_A = x,\ PuK_A = a;$ $\quad$ $\mathcal{B}: PrK_B = y,\ PuK_B = b;$ $\quad$ $\mathcal{E}: PrK_C = z,\ PuK_C = e;$

$b, e;\ \ a = g^x \bmod p$ $\quad$ $a, e;\ b = g^y \bmod p;$ $\quad$ $a, b;\ e = ---$

ElGamal encryption

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

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

message to be encrypted

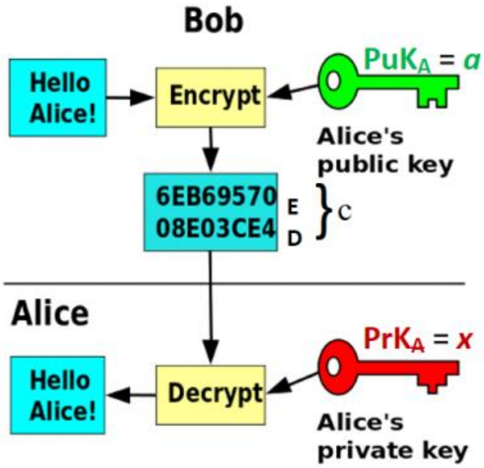
$i \leftarrow \text{randi};\ \ i \in \mathbb{Z}_{p-1} = \{0, 1, 2, ..., p-2\}$

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

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

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

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



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

$$D^{-x} = D^{p-1-x} \bmod p$$

D^{-x} computation

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

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

$m_i \in \{1, 2\} \vee m \in \{n_1, n_2\}$.

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

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

$$\left.\begin{array}{l} E_{1A} = m_1 \cdot a^{i_1} \bmod p;\ D_{1A} = g^{i_1} \bmod p \\ E_{2A} = m_2 \cdot a^{i_2} \bmod p;\ D_{2A} = g^{i_2} \bmod p \end{array}\right\} \xrightarrow{C_{1A},\ C_{2A}}$$

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

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

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

$$Enc(b, i_3, E_{2A}) = (E_{2AB}, D_{2AB}) = C_{2AB}$$

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

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

$$C_{iAB} = (E_{iA} \cdot b^{r_3} \bmod p,\ g^{r_3} \bmod p)$$

A: $\xleftarrow{\quad\quad}$

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

$$= \frac{E_{2A} \cdot b^{r_3}}{(g^i)^x} = \frac{m_2 \cdot a^i \cdot b^{i_3}}{g^{i_2 x}} =$$

If $i = 2 \rightarrow m_i = 2$

If $i = 2 \rightarrow m_i = 2$

$$= \frac{m_2 \cdot a^{i_2} \cdot b^{i_3}}{g^{i_2 x}} = \frac{m_2 \cdot \cancel{g^{x i_2}} \cdot b^{i_3}}{\cancel{g^{i_2 x}}} =$$

$$= m_2 \cdot b^{i_3} = E_{2ABA} \xrightarrow{E_{2ABA}} \mathcal{B}: \; C_{2ABA} = (E_{2ABA}, D_{2AB})$$

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

$$Dec(y, c_{iABA}) =$$

$$= \frac{E_{iABA}}{(D_{iAB})^{y}} = \frac{m_2 \cdot b^{i_3}}{(g^{i_3})^{y}} = \frac{m_2 \cdot (g^{y})^{i_3}}{g^{i_3 y}} =$$

$$= \frac{m_2 \cdot \cancel{g^{y i_3}}}{\cancel{g^{i_3 y}}} = m_2$$

$$\xleftarrow{m_2,\, i_3}$$

$$m_i = E_{iABA} \cdot (b)^{-i_3} \bmod p =$$

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

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

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

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

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

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

(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.

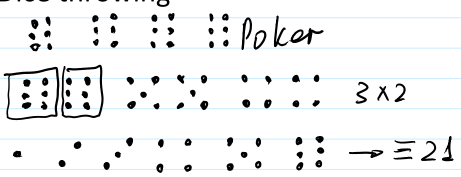
$$i_3 \leftarrow randi(\mathcal{Z}_{p-1})$$

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

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

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

Dice throwing



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

$r_1 \leftarrow randi, \ldots, r_6 \leftarrow randi$

$c_i = Enc(a, r_i, m_i), i = \overline{1,6}.$

$c_1 \equiv 1;\ c_2 \equiv 2;\ c_3 \equiv 3; \ldots c_6 \equiv 6.$ $\longrightarrow$ $B: c_i \leftarrow rand\{c_i\}$

$\longrightarrow$ $C: c_i = c_6$

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

$i = \overline{1,6}$ kauliuko reikšmės

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

Card game - Poker

52 kortos & 4 mastis

1 kortos šifrav.

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

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