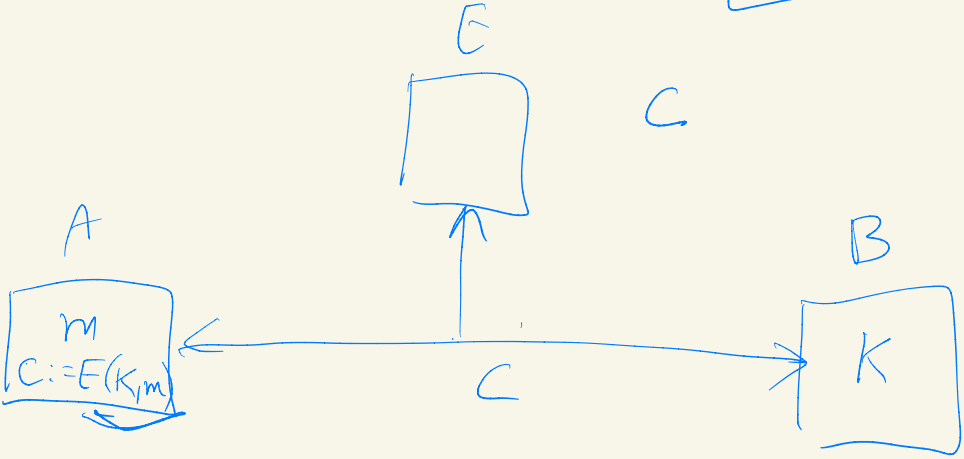
23-3-21



m : texto plano

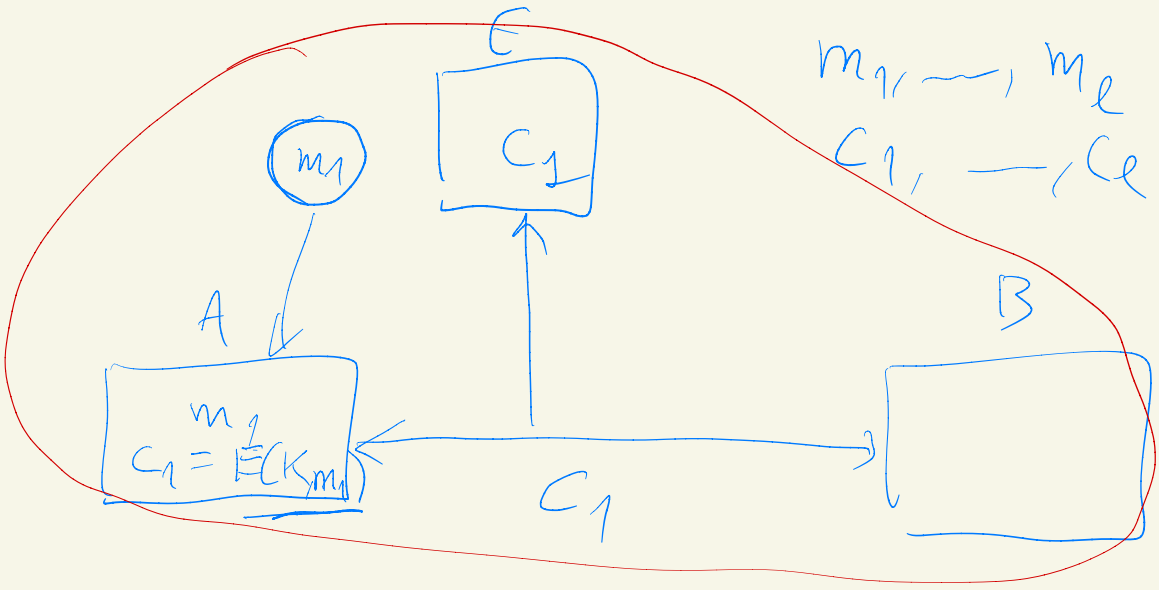
C : texto cifrado

- texto cifrado : C
- texto plano : (m, c)

C'

- texto plano elegido

$m_1, \dots, m_\ell$ $\quad c_i = E(K, m_i)$



- **Texto cifrado elegido**

E puede elegir $m_1, \dots, m_r, c_{r+1}, \dots, c_{r+s}$

$c_i := E(K, m_i) \quad 1 \le i \le r$

$m_j := D(K, c_j) \quad r+1 \le j \le r+s$

$K_1 \qquad a_1 = h(K_1, m)$

A $\longleftrightarrow$ B

K_1 $\qquad$ K_1

K_1

K_2

64

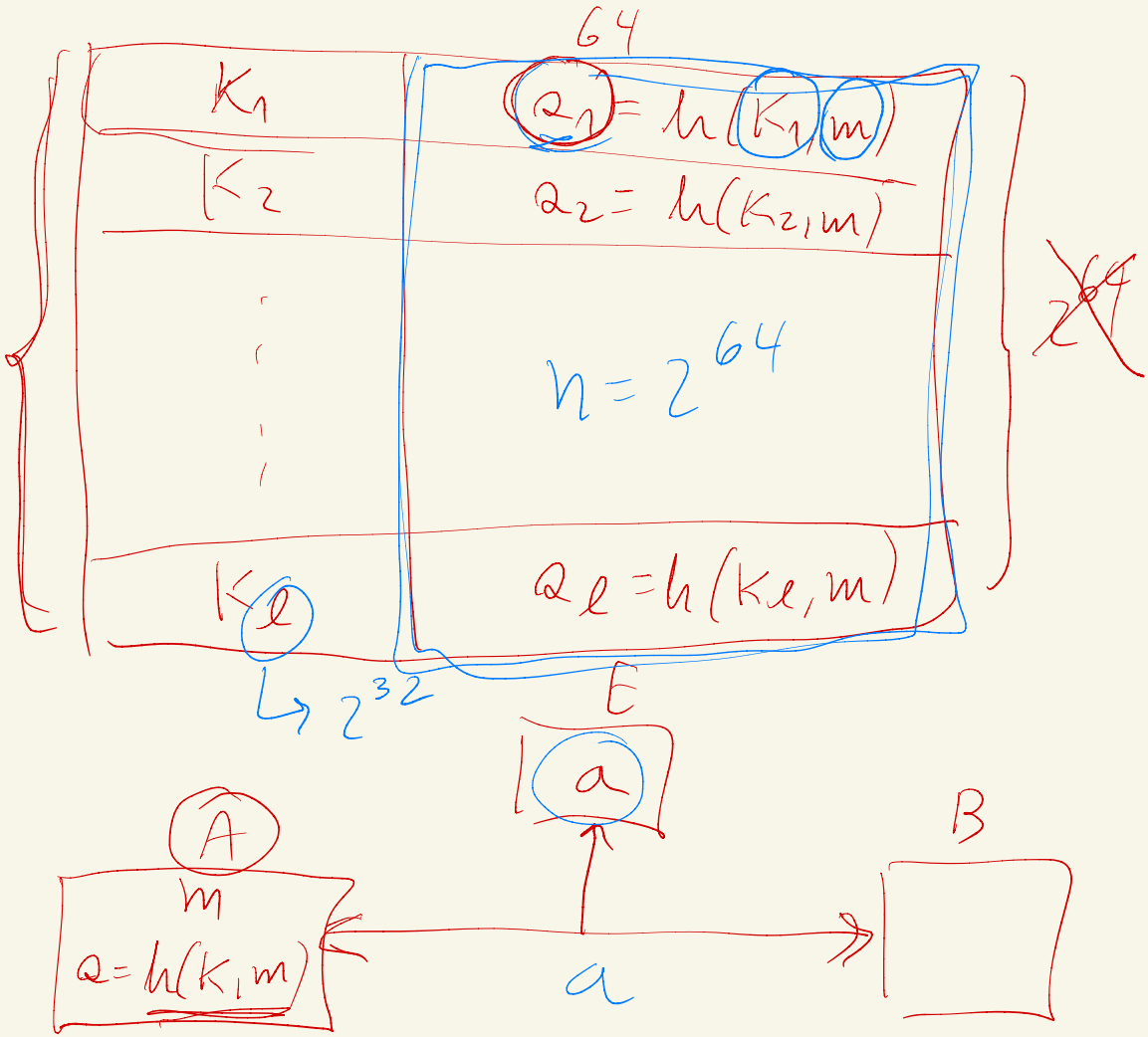
2^{64}

$a_1 = h(K_1, m)$

$a_2 = h(K_2, m)$

$a_1 = h(K_1 \; m)$

$d\,h(K, m) = a_1$?



$q = q_3$

$h(K, m) = h(K_3, m)$

$q_2 = q_5$

$h(K_2, m) = h(K_5, m)$

Pr (k personas nacieron en días distintos)

$$= \left(\frac{365-0}{365}\right)\left(\frac{365-1}{365}\right)\left(\frac{365-2}{365}\right)\cdots\left(\frac{365-(k-1)}{365}\right)$$

$1 \quad 2 \quad 3 \quad k$

$Pr(X = l)$

$$Pr(X=4) = \left(\frac{365-1}{365}\right)\cdot\left(\frac{365-2}{365}\right)\cdot\frac{3}{365}$$

$Pr(X=1) = 0$

$$Pr(X=4) = \left(\frac{n-0}{n}\right)\left(\frac{n-1}{n}\right)\left(\frac{n-2}{n}\right)\cdot\frac{3}{n}$$

$1 \quad 2 \quad 3 \quad 4$

$$Pr(X=4) = (1-p)^3 \cdot p$$

$$Pr(X=n+1) = \left(\frac{n-0}{n}\right)\left(\frac{n-1}{n}\right)\cdots\left(\frac{n-(k-1)}{n}\right)$$

$1 \quad 2 \quad 3 \quad \cdots \quad k$

$$\left(\frac{1}{n}\right)^{n} \cdot 1$$

$n \qquad n+1$

$$Pr(X=k) = \left(\prod_{i=1}^{k-1}\left(\frac{n-(i-1)}{n}\right)\right)\cdot\frac{k-1}{n}$$

$$Pr(X=n+2) = 0$$

$$E[X] \simeq \sqrt{n}$$