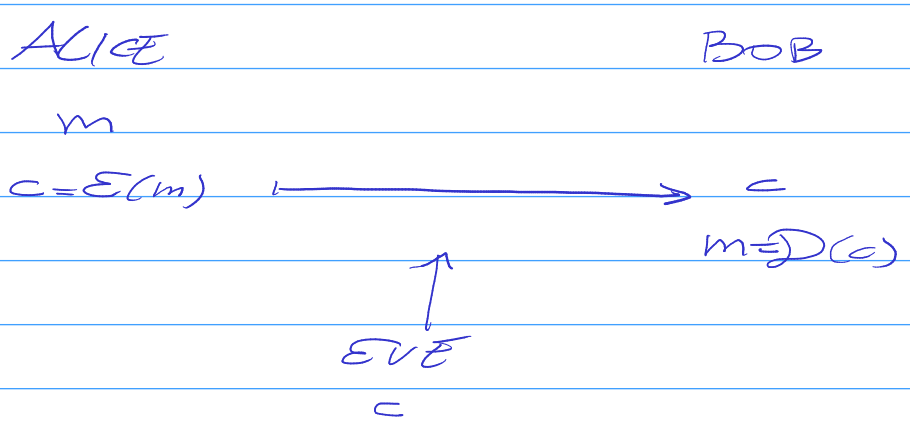
CRITTOGRAFIA

→ confidenzialità



CRITTOSISTEMA PERFETTO → $P_E(m'=m) = P_E(m'=m|c)$

Esempio

ALICE	K_1	K_2
0	0	1
1	1	0

BOB conosce K_i, riceve $c=1$ → $i=1$, $m=1$; $i=2$, $m=0$

EVE può indovinare con $p=\frac{1}{2}$
(anche se non ha visto c).

ALICE	K_1	K_2
00	00	11
01	01	10
10	10	01
11	11	00

$c=10$

BOB → $i=1$, $m=10$; $i=2$, $m=01$

EVE → esclude i messaggi
00 11

probabilità di indovinare m visto $c = \frac{1}{2}$
senza $c = \frac{1}{4}$

ALICE	00	01	10	11	BOB
00	00	01	10	11	
01	01	00	11	10	
10	10	11	00	01	
11	11	10	01	00	

00 è codifica possibile di qualsiasi messaggio

$|K| = |M|$

CRITTOSISTEMA: coppia di algoritmi

$$E: M \times K \to C$$
$$D: C \times K \to M$$

tali che

$$\forall k \in K \; \exists k' \in K : \forall m \in M : D(E(m,k),k') = m$$

le chiavi non dipendono dai messaggi

OSS: $|C| \geq |M|$ (per una chiave fissata messaggi diversi hanno codifiche diverse).

Teorema: Un crittosistema perfetto (*) deve avere $|K| \geq |M|$

DIM: Se $|K| < |M|$ $\forall m \in M$ $\exists$ almeno un resto cifrato $c \in C$ tale che $\forall k \in K$, $E(m,k) \neq c$

$\Rightarrow$ dato c si può escludere almeno un messaggio m in chiaro.