CRYPTOGRAPHY

PROF. VENTURI

The art and science of SECURE COMMUNICATION.

An ancient discipline.

Crypto as a SCIENCE: (1949 – TODAY)

- Definitions of security
- Proofs of security.

) PROVABLE SECURITY

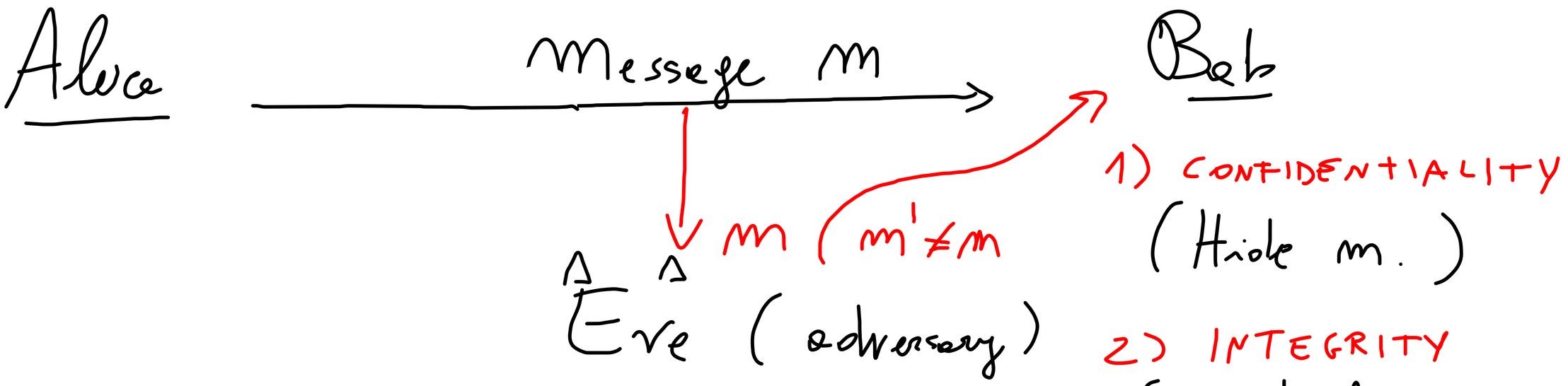
Not cover:

- Coding
- Security of HW/SW
- Hacking.

EXAM: Written ~ 3 HOURS
3 EX + 1 OPEN QUESTION
No Books/Notes

Textbook: KATZ-LINDELL

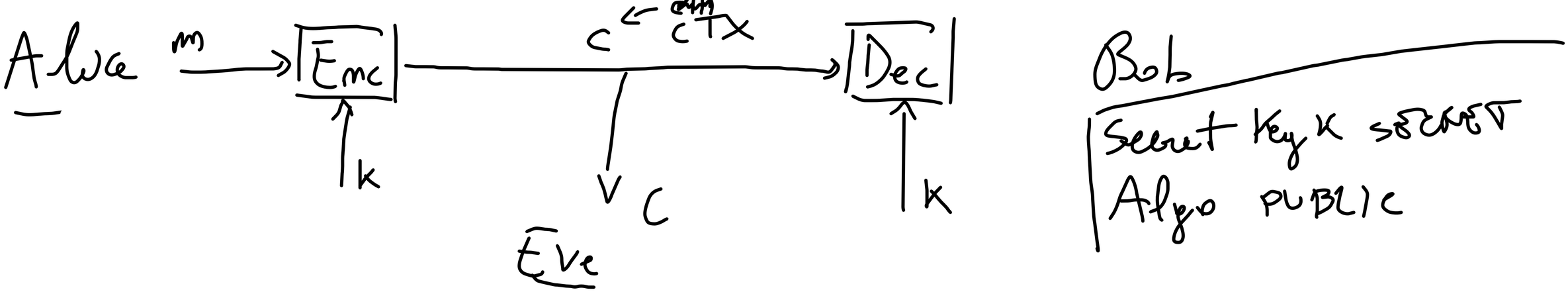
SECURE COMMUNICATION



1) CONFIDENTIALITY
(Hide m.)

2) INTEGRITY
(Cannot change m to m' ≠ m.)

Let's start with PERFECT SECRECY (Shannon, 49')
He was the first to model SYMMETRIC ENCRYPTION.



- $Enc : \mathcal{M} \times \mathcal{K} \to \mathcal{C}$
- $Dec : \mathcal{C} \times \mathcal{K} \to \mathcal{M}$

Assumption: $k \in \mathcal{K}$

RANDOM! $k \leftarrow\!\!\$\ \mathcal{K}$

e.g. $\mathcal{K} = \{0,1\}^n$

DEF. (CORRECTNESS). $\Pi = (Enc, Dec)$ is CORRECT if:

$\forall k \in \mathcal{K}, \forall m \in \mathcal{M}$: $Dec(k, Enc(k, m)) = m$.

DEF. (PERFECT SECRECY) Let M be any distribution on $\mathcal{M}$.
Let K be UNIFORM over $\mathcal{K}$ and $C = Enc(K, M)$.
$\Pi = (Enc, Dec)$ is perfectly secret if:

$\forall M, \forall m \in \mathcal{M}, c \in \mathcal{C}$: $Pr[M = m] = Pr[M = m \mid C = c]$.

Very strong: CTX reveals nothing about PTX!

UNCONDITIONAL!

THM. The following are equivalent:

(i) PERFECT SECRECY $\left(\Pr[M=m] = \Pr[M=m \mid C=c] \right)$

(ii) M and C are <u>independent</u> $\left(I(M;C) = 0 \right)$

(iii) $\forall m, m' \in \mathcal{M}, \forall c \in \mathcal{C}: \Pr[Enc(K,m)=c] = \Pr[Enc(K,m')=c]$

Proof. (i) $\Rightarrow$ (ii)

$$\Pr[M=m] = \Pr[M=m \mid C=c] \qquad \text{(by (i))}$$

$$= \frac{\Pr[M=m \wedge C=c]}{\Pr[C=c]} \qquad \text{(by Bayes)}$$

$$\Rightarrow \Pr[M=m \wedge C=c] = \Pr[M=m] \cdot \Pr[C=c] \quad \blacksquare$$

(ii) $\Rightarrow$ (iii) Take $m \in \mathcal{M}$, $c \in \mathcal{C}$:

$$\Pr[Enc(K,m) = c] = \Pr[Enc(K,M) = c \mid M = m]$$

$$= \Pr[C = c \mid M = m]$$

$$= \Pr[C = c] \quad \text{(by (ii))}$$

(C = $Enc(K,M)$)

Also, $\forall m' \in \mathcal{M}$: $\Pr[Enc(K,m') = c] = \Pr[C = c]$ ∎

(iii) $\Rightarrow$ (i) Fix any $c \in \mathcal{C}$:

$$\Pr[C = c] = \sum_{m} \Pr[C = c \wedge M = m'] \quad \text{(set theory)}$$

$$= \sum_{m'} \Pr[C = c \mid M = m'] \cdot \Pr[M = m'] \quad \text{(Bayes)}$$

$$= \sum_{m'} \Pr[Enc(K,M) = c \mid M = m'] \cdot \Pr[M = m'].$$

$$= \sum_{m'} \Pr[\mathrm{Enc}(K, m') = c] \cdot \Pr[M = m']$$

$$= \sum_{m'} \Pr[\mathrm{Enc}(K, m) = c] \cdot \Pr[M = m'] \quad (\text{by (iii)})$$

$$= \Pr[\mathrm{Enc}(K, m) = c] \cdot \underbrace{\sum_{m'} \Pr[M = m']}_{= 1}$$

$$= \Pr[\mathrm{Enc}(K, m) = c]$$

$$= \Pr[\mathrm{Enc}(K, M) = c \mid M = m] = \Pr[C = c \mid M = m].$$

$$\Rightarrow \boxed{\Pr[C = c] = \Pr[C = c \mid M = m]}.$$

Now: $\Pr[M = m \mid C = c] \cdot \Pr[C = c] = \Pr[M = m \wedge C = c]$

$$= \Pr[C = c \mid M = m] \cdot \Pr[M = m]$$

$$\Pr[M=m] = \frac{\Pr[M=m \mid C=c] \cdot \Pr[C=c]}{\Pr[C=c \mid M=m]}$$

$$= \Pr[M=m \mid C=c] \qquad \blacksquare$$

(OTP)
ONE-TIME PAD . $\Pi = (Enc, Dec)$: $K = M = C = \{0,1\}^n$

- $Enc(k,m) = k \oplus m = c$

$$\begin{array}{r} 01010 \\ 11100 \\ \hline 10110 \end{array} \oplus$$

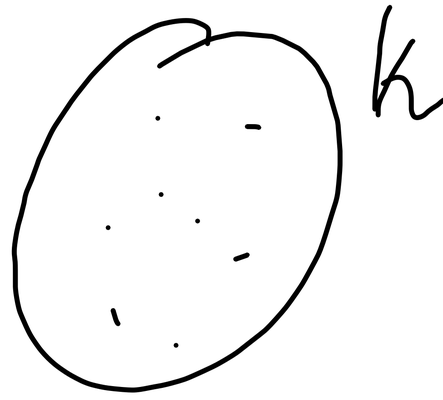
- $Dec(k,c) = c \oplus k = (m \oplus k) \oplus k = m$!

COR . The OTP is PERFECTLY SECRET.

Proof. Fix $m \in \{0,1\}^n$, $c \in \{0,1\}^n$

$$\Pr[Enc(K,m) = c] = \Pr[K \oplus m = c]$$

$$= \Pr[K = c \oplus m] = 2^{-n}$$



Fix $m' \in M$ $\Pr[Enc(K,m') = c] = 2^{-n}$ ∎

There are limitations:

THOSE ARE INHERENT.

- Key as long as msg! ←
- Key can be used only once!

Say Eve knows (m, c) s.t. $k \oplus m = c$

If $c' = k \oplus m'$. Now: $c \oplus c' = m \oplus m'$

THM (Shannon). In any PERFECTLY SECRET secret-key encryption, we have $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof. Take M to be uniform over $\mathcal{M}$. Take any $c \in \mathcal{C}$ s.t. $\Pr[C = c] > 0$.

Consider $\mathcal{M}' = \{ Dec(k, c) : k \in \mathcal{K} \}$.

Assume $|\mathcal{K}| < |\mathcal{M}|$

Then: $|\mathcal{M}'| \leq |\mathcal{K}| < |\mathcal{M}|$

There exists $m \in \mathcal{M} \setminus \mathcal{M}'$. But now:

$\Pr[M = m] = 1/|\mathcal{M}| \neq$

$\Pr[M = m \mid C = c] = 0$

∎

Main question for us: Can we have "secure" SKE

s.t. : 1) $|k| << |m|$

2) Same k for all msg.