# CRYPTOGRAPHY

Schedule: Tuesday 8-11 (AULA MAGNA)
Friday 11-13 (AULA 1C)

Website: dventura83.github.io

Exam: Written. 3 hours. A mix of exercises and theory.

Made with Goodnotes

# INTRODUCTION

Main focus: Modern cryptography.

Modern: From art to science.

In the past: Secret communication.

Today: Security in digital apps.

Science: Precise definitions of security and proofs of security.

Best thing: Prove cryptosystem X is secure (under NO ASSUMPTIONS).

Next best thing: As above but under some assumptions.

Made with Goodnotes

**Assumptions:** Hardness of some well-studied computational task.

$\hookrightarrow$ Attacker is efficient (not unlimited computational power).

There are hard problems : $P \neq NP$

Think of some problem that we don't know how to solve efficiently:

$$n = p \cdot q \qquad p, q \text{ primes}$$

**FACTORING:** given $n$ $\qquad |p| = |q| \approx \lambda$ bits

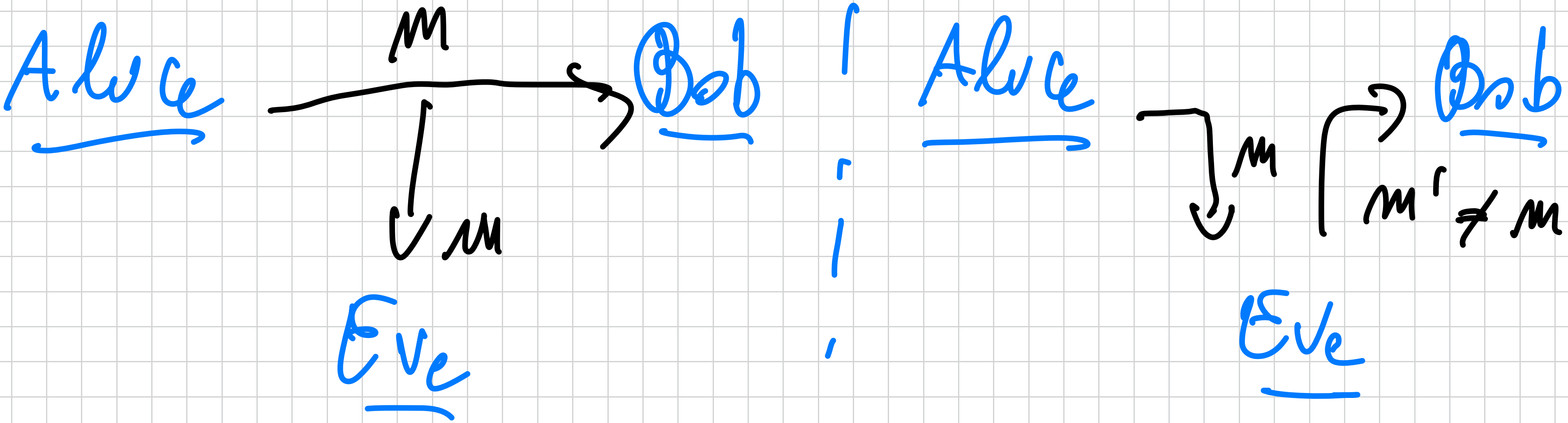
find $p, q$ ; $\lambda = 2048$

Made with Goodnotes

Goal : Prove X (encryption) is "secure" if problem Y is HARD.

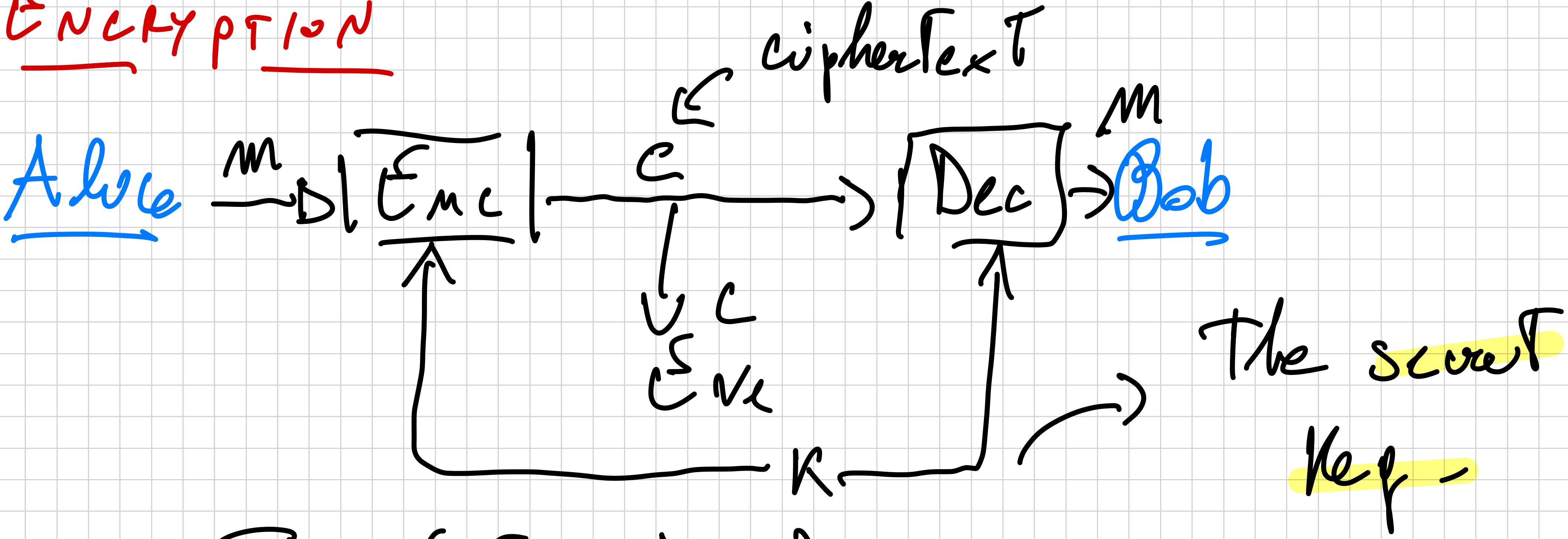
↳ If ∃ efficient A breaking X, then ∃ efficient M breaking Y.

What X? Secure communication.



Made with Goodnotes

# ENCRYPTION



$X = \Pi = (Enc, Dec)$

Kerchoff principle : Algorithms must be public!

Secret Key Encryption $\Pi = (Enc, Dec)$

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

Made with Goodnotes

$\mathcal{K}$ = Key space; $\mathcal{M}$ = Message space

$\mathcal{C}$ = CipherText space.

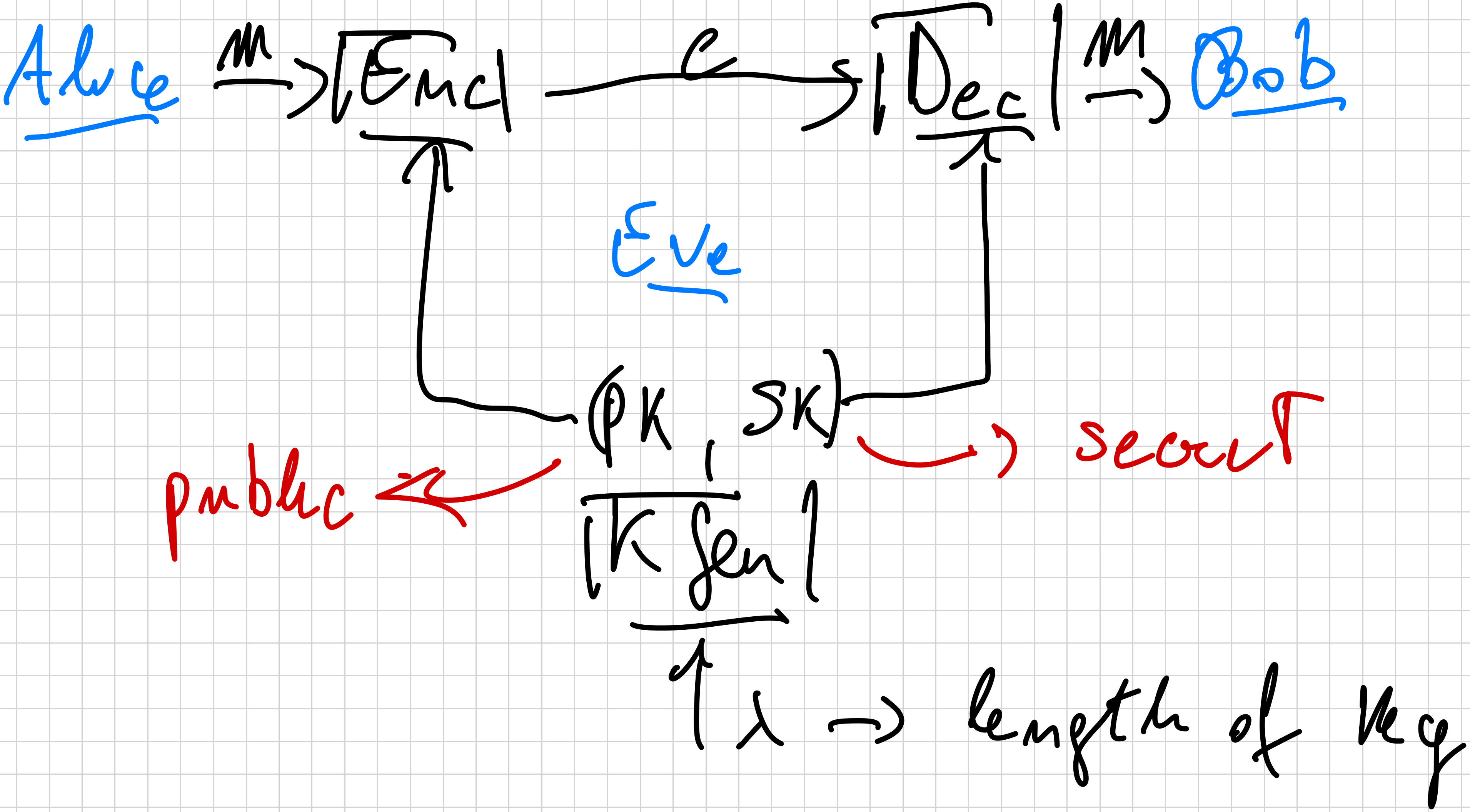
**Correctness**: $\forall k \in \mathcal{K}, \forall m \in \mathcal{M}$

$$Dec(k, Enc(k, m)) = m$$

**Security**: ??? Note that for sure $k \in \mathcal{K}$ must be "RANDOM" and SECRET

**Problem**: Keys must be secret and shared.

Made with Goodnotes

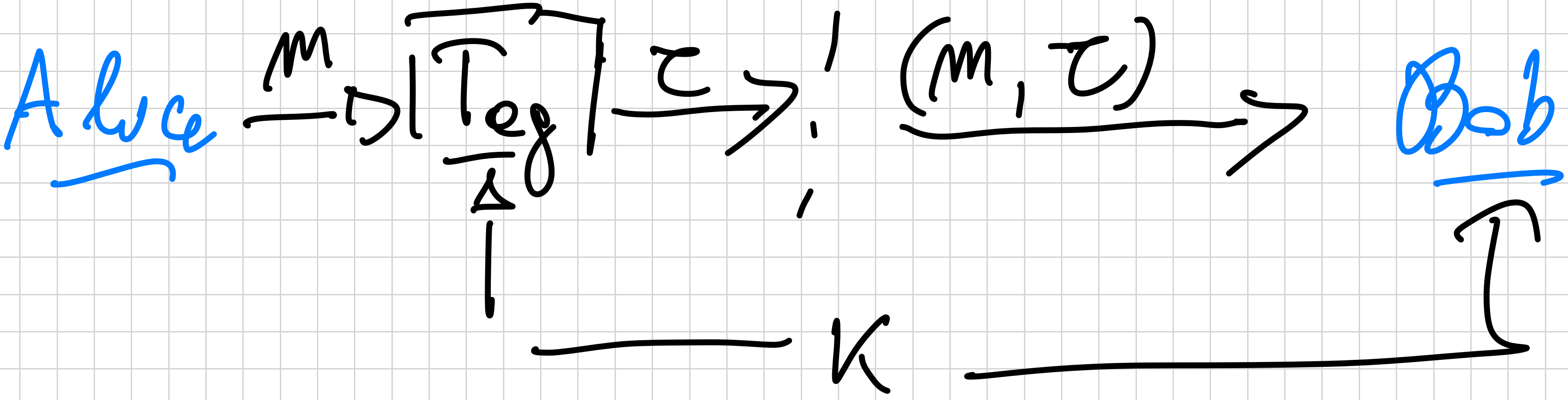


Public-key encryption (PKE)

$\Pi = (\mathrm{KGen}, \mathrm{Enc}, \mathrm{Dec})$

Problem: Public keys must be authentic!

# AUTHENTICATION

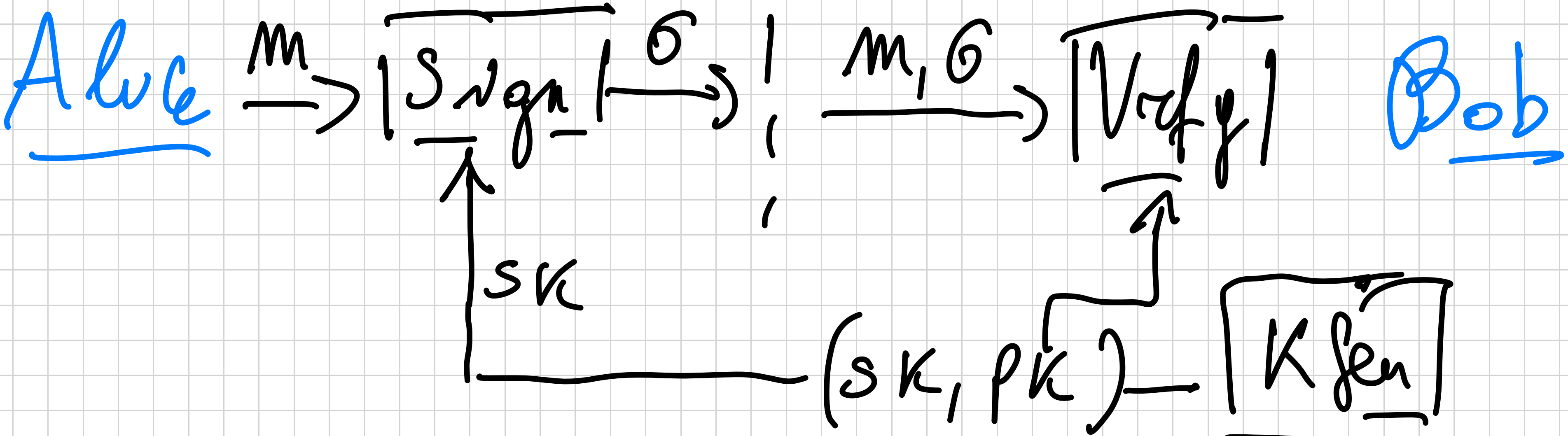


$$\text{Tag} : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$$

Verify :

$$\begin{tikzcd} m \arrow[r] & \boxed{\text{Tag}} \arrow[r] & \tau' \overset{?}{=} \tau \\ & K \arrow[u] & \end{tikzcd}$$

MESSAGE AUTHENTICATION CODE (MAC)



$$\mathrm{Sign}: \mathcal{SK} \times \mathcal{M} \to \mathcal{S}$$

$$\mathrm{Vrfy}: \mathcal{PK} \times \mathcal{M} \times \mathcal{S} \to \{\overset{\text{REJECT}}{0}, \overset{\text{ACCEPT}}{1}\}$$

$$\Pi = (\mathrm{KGen}, \mathrm{Sign}, \mathrm{Vrfy})$$

DIGITAL SIGNATURE

# PERFECT SECRECY

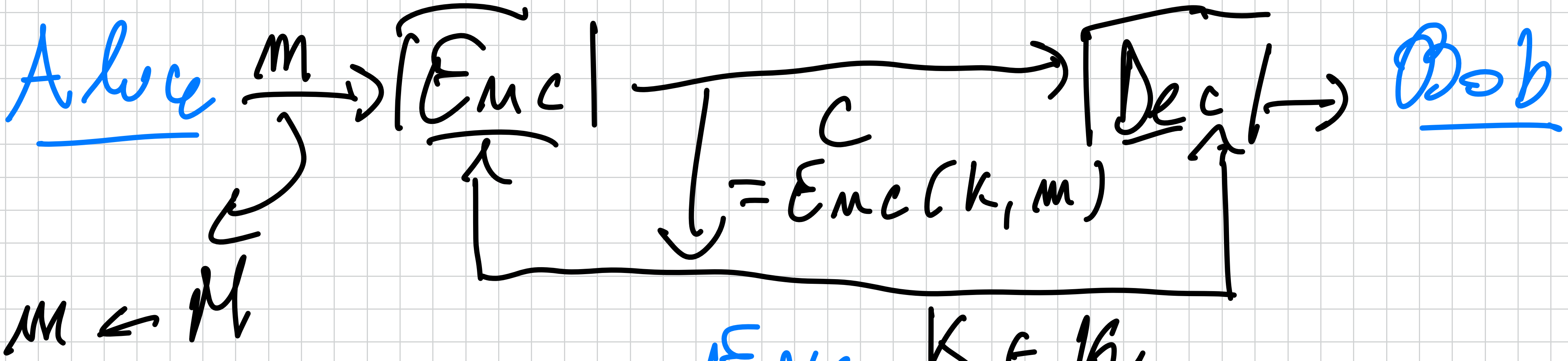
Information-theoretic treatment of SKE. (unconditional security).

**Def.** (Shannon '49). Let $M$ be a distribution over $\mathcal{M}$, and $K$ be uniform over $\mathcal{K}$. (Then, $C = \mathrm{Enc}(K,M)$ is also a distribution.). We say $\Pi = (\mathrm{Enc}, \mathrm{Dec})$ is PERFECTLY SECRET if: $\forall\, M$, $\forall\, m \in \mathcal{M}$, $\forall\, c \in \mathcal{C}$ :

$\mathrm{Enc}(K,M)$

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

Made with Goodnotes



Eve

$K \in \mathcal{K}$

↳ $k \leftarrow K$ (UNIFORM

$\mathcal{C}$

$\mathcal{C}, \mathcal{M}$

Intuition: A priori prob. that $M = m$ is same as a posterior prob. that $M = m$ given that $C = \mathrm{Enc}(K, M = m) = c$.

Next time: This notion is achievable at high price: Key as long as message and can be used once.

$$Enc(K, m) = K \oplus m = c$$

$$\mathcal{C} = \mathcal{K} = \mathcal{M} = \{0,1\}^n$$

Made with Goodnotes