CRYPTO

Webpage: Just google for my name.

DANIELE VENTURI.

EXAM: Written. No books. No phones :)

3 parts: 1 exercise, 1 theory question.

Book: Katz, Lindell. Intro to modern cryptography.

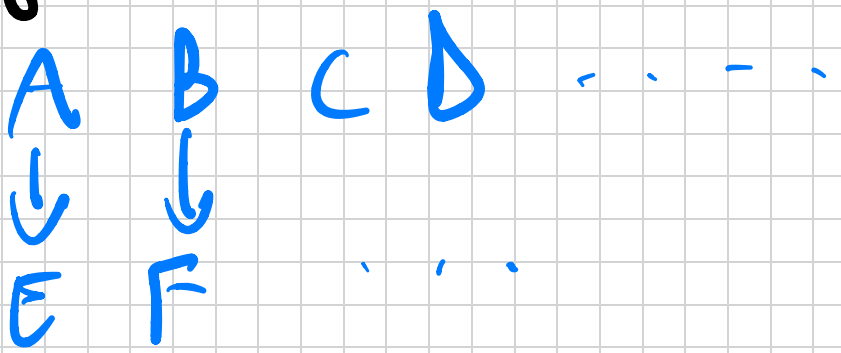
INTRO

What this course is about?

An intro to MODERN CRYPTO.

Why modern? Because the way crypto is done today is DIFFERENT from the past.

It exists for multiple. Secure communication.



Before the '50s : Crypto was an ART.
Secure until not broken.
Famous example : TLS.
Modern crypto : Crypto as a SCIENCE :
- Precise definitions !
- Proofs !
Turing Award : Silvio MICALI
Shafi GOLDWASSER
Two flavors : UNCONDITIONAL PROOFS
CONDITIONAL PROOFS.

Unconditional: No conditions (assumptions)
Possible, but INEFFICIENT.
Conditional: Assumptions! Like: $P \neq NP$.
There exist problems that seem to be hard for efficient computation.

EXAMPLE: FACTORING.

$n = p \cdot q$; p, q PRIMES

$|p| \approx |q| \approx \lambda$ bits

λ SEC. PARAM.

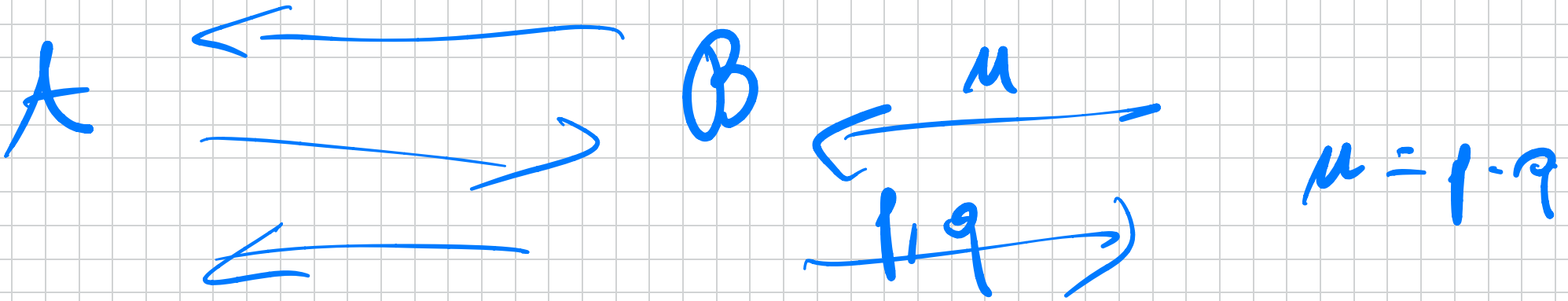
$\lambda = 1024$

Hard to compute p, q given n.

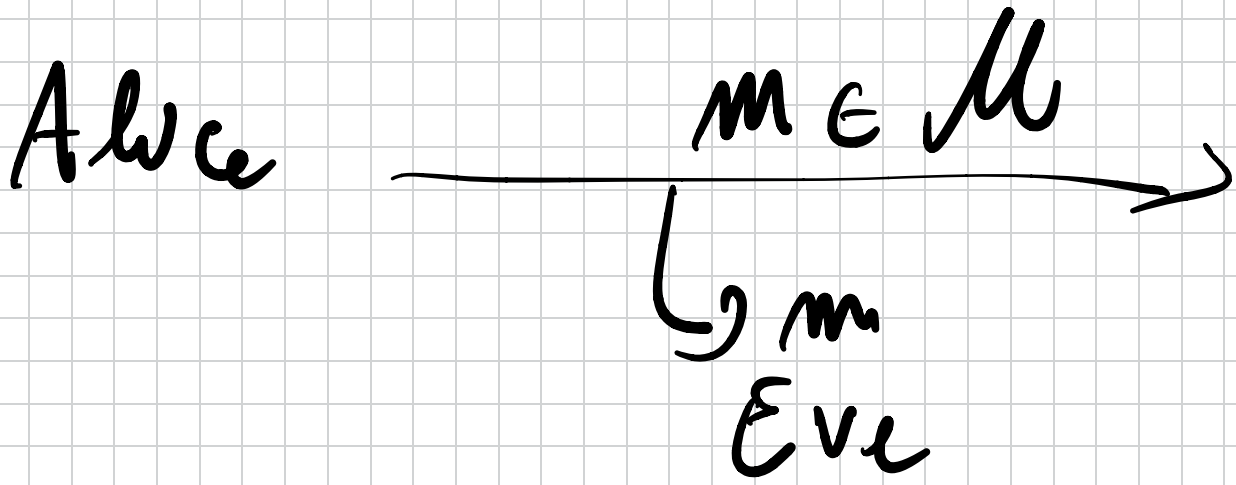
Recipe for PROVABLE SECURITY. Prove thus:

THM. Cryptosystem X is "SECURE" if FACTORING is HARD.

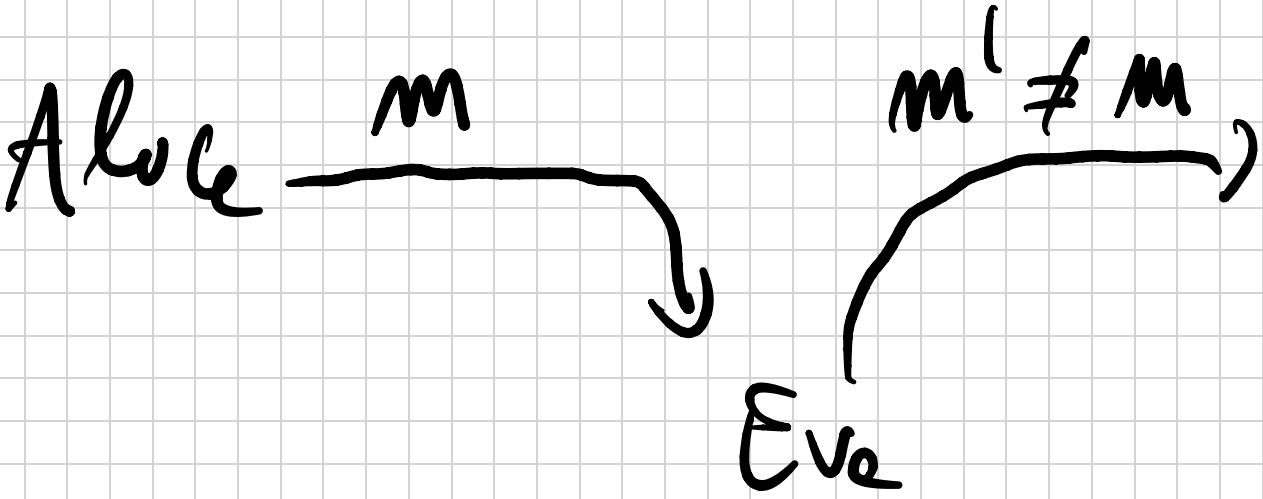
Assume X NOT secure: $\exists$ efficient machine A "BREAKING" X. Then $\exists$ efficient machine B solving FACTORING



SECURE COMMUNICATION



① CONFIDENTIAL COMMUNICATION



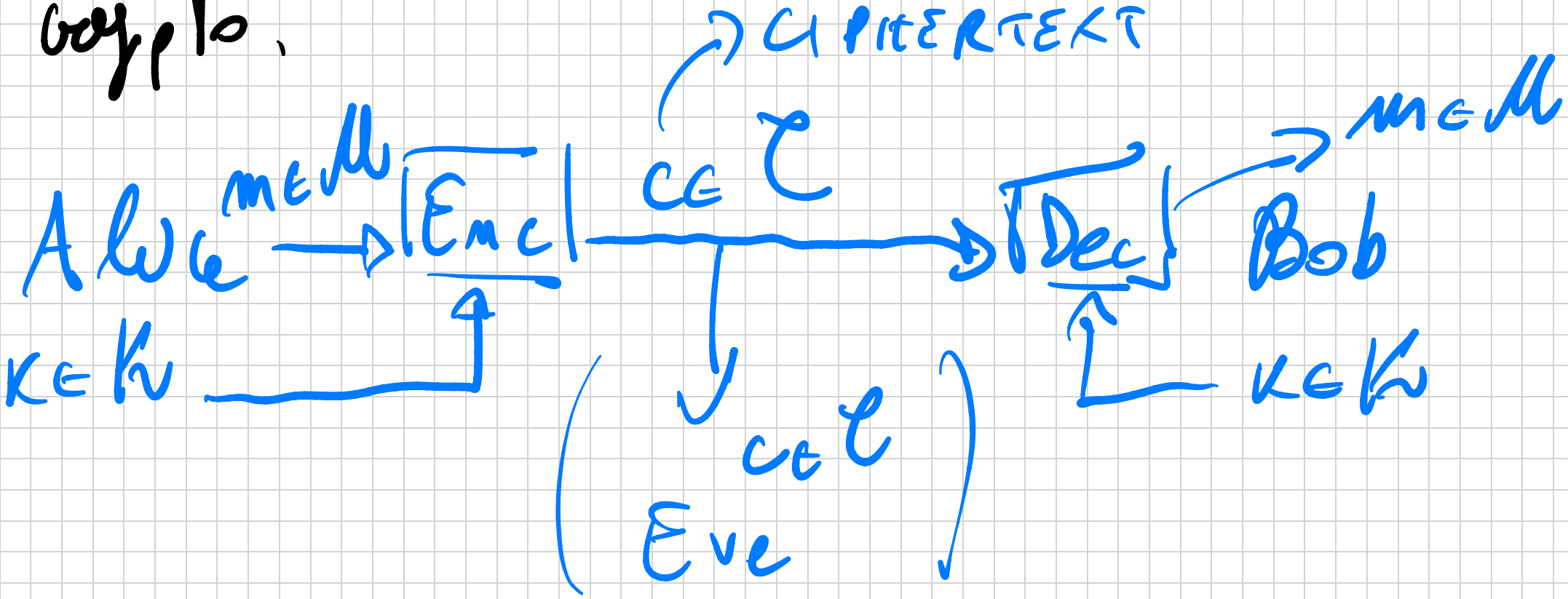
② MESSAGE INTEGRITY

We will cover 2 approaches:

- SYMMETRIC CRYPTO: Alice and Bob share a key $K \in \mathcal{K}$; the key is RANDOM and unknown to Eve.
- ASYMMETRIC CRYPTO: Alice and Bob do NOT share a key, but they have each their own key pair (pk, sk) where pk PUBLIC and sk SECRET.

UNCONDITIONAL SECURITY

We start with GOAL ① in symmetric crypto.



Symmetric encryption SKE: $\Pi = (Enc, Dec)$ such that:

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

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

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

Kerckhoff: Security only should depend on secrecy of the key, not of algorithms.

Shannon (1950): Put forward a definition called PERFECT SECRECY.

Def Let M be any distribution over $\mathcal{M}$, and K be uniform over $\mathcal{K}$. (Then observe that $C = Enc(K, M)$ is a distribution over $\mathcal{C}$.)

We say $(Enc, Dec) = \Pi$ is PERFECTLY SECRET if $\forall M$, $\forall m \in \mathcal{M}$, $\forall c \in \mathcal{C}$:

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

Intuition: Ciphertext C reveals nothing on plaintext m, besides what you knew already.

Shannon did two things:

1) The definition is achievable.

2) It comes with INHERENT limitations in practice.

LEMMA. The following are equivalent:

(I) PERFECT SECRECY.

(II) M and C are INDEPENDENT.

(III) $\forall\, m, m' \in \mathcal{M}$, $\forall\, c \in \mathcal{C}$:

$$\Pr_K[Enc(K, m) = c] = \Pr_K[Enc(K, m') = c]$$

$\subseteq_2$ $K \equiv$ UNIFORM over $\mathcal{K}$.

Let's take it for granted. Now here is how to get PERFECT SECRECY.

The ONE-TIME PAD: $K = M = C = \{0,1\}^n$

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

$$\begin{array}{r} k = 0\,1\,1 \\ m = 1\,0\,1 \quad \oplus \\ \hline c = 1\,1\,0 \end{array}$$

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

$= m$ ✓

Thm. OTP is perfectly secret.

Proof. We use def. (2.2) in the above lemma. Well, for any $m, m' \in \mathcal{M}$ and $c \in \mathcal{C}$:

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

$$= \Pr_K[K \oplus m = c]$$

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

For the same argument:

$$Pr[Enc(K, m') = c] = 2^{-n}. \quad \square$$

There seem to be limitations:

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

In fact, assume we encrypt m_1, m_2 with K. Then:

$$c_1 = K \oplus m_1; \; c_2 = K \oplus m_2$$

$$c_1 \oplus c_2 = m_1 \oplus m_2$$

If I know single pair (m_1, c_1) can compute m_2.

Thm (Shannon). Let Π be ANY PERFECTLY SECRET SKE, then

$$|K| \geq |M|.$$

Proof. Take M to be UNIFORM over M. Take any c s.t. $Pr[C=c] > 0$.

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

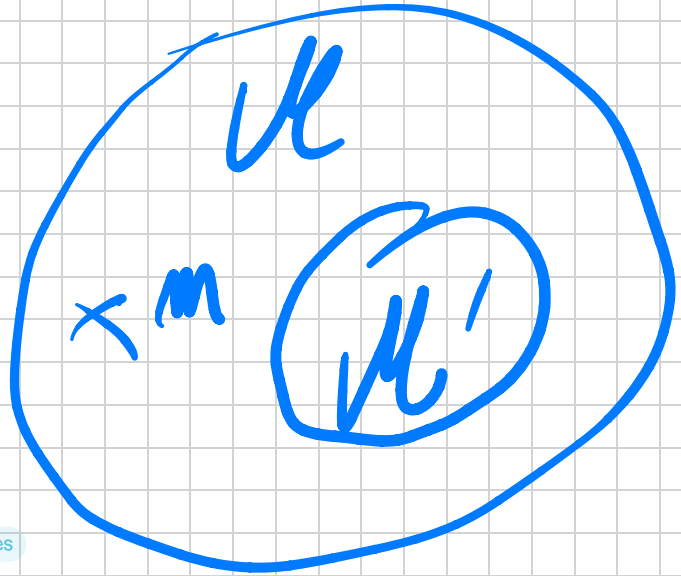
Consider $\mathcal{M}' = \{ Dec(K, c) : K \in \mathcal{K} \}$

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

Then:

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

$$\Rightarrow |\mathcal{M}'| < |\mathcal{M}|$$



$$\Rightarrow \exists\ m \in \mathcal{M} \setminus \mathcal{M}'$$

Now:

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

On the other hand:

$$\Pr[M = m \mid C = c] = 0$$ ∎