# NANO COURSE
# ON
# THEORETICAL CRYPTOGRAPHY

---

IIT GANDHINAGAR (21-26 DECEMBER 2023)

VENKATA KOPPULA (IITD)

# COURSE OBJECTIVES

- A glimpse of ‘provable security’
  - Until the middle of 20th century, security was mostly ‘ad-hoc’
  - Today, we have provable guarantees for a lot of the security systems used in practice

le chiffrage
indéchiffrable

- This course: 3-step recipe for some popular security goals
  - Formal definition
  - Construction
  - Security proof for construction

# A BRIEF HISTORY

Starts after the WW2 action

# A BRIEF HISTORY OF MODERN CRYPTOGRAPHY

## 1949: The first 'crypto proof'

CLAUDE SHANNON

Studied 'perfectly secure' encryption schemes

the real 'le chiffrage indechiffrable'

Constructions and limitations of perfect security

# A BRIEF HISTORY OF MODERN CRYPTOGRAPHY

## Early 1970s: The first 'encryption standard', and developments in complexity theory

Data Encryption Standard was proposed (IBM + NSA)

Richard Karp

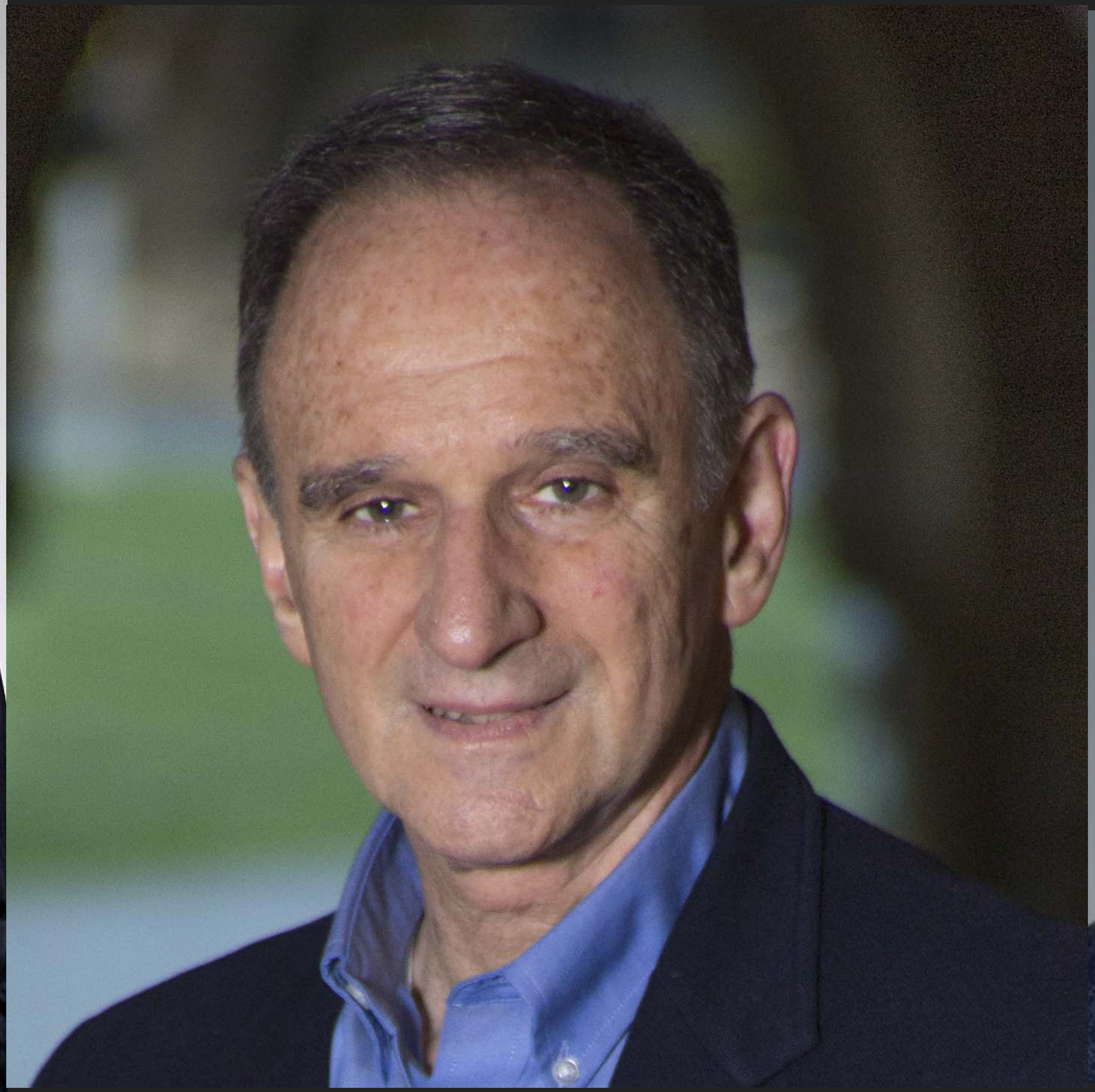
Steven Cook

Developed theory of polynomial reductions, NP hardness

# A BRIEF HISTORY OF MODERN CRYPTOGRAPHY

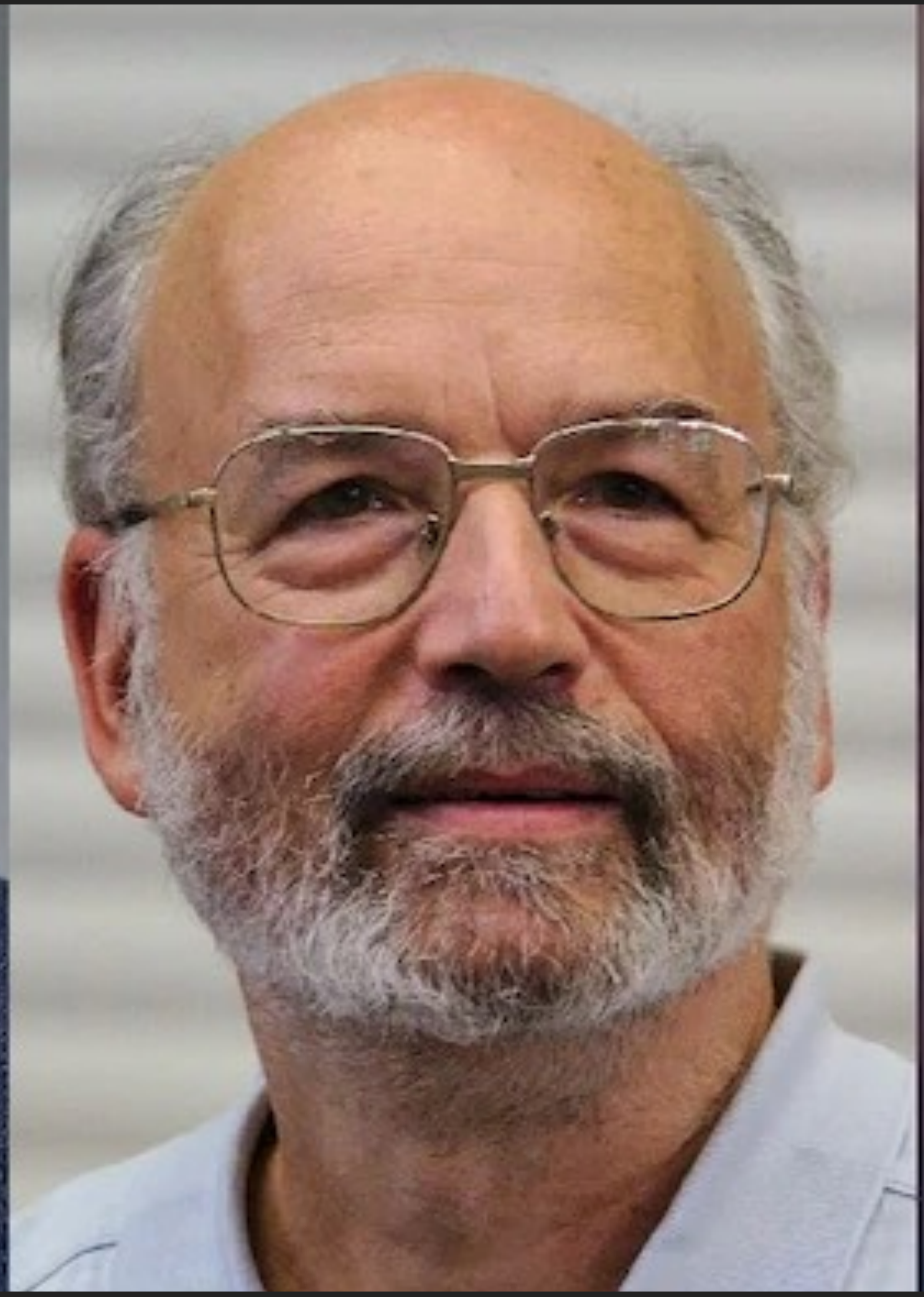
Late 1970s: Crypto goes from ‘private’ to ‘public’

Whitfield
Diffie



Martin
Hellman

Ron
Rivest



Adi
Shamir

Leonard
Adleman

CRYPTO WARS

# A BRIEF HISTORY OF MODERN CRYPTOGRAPHY

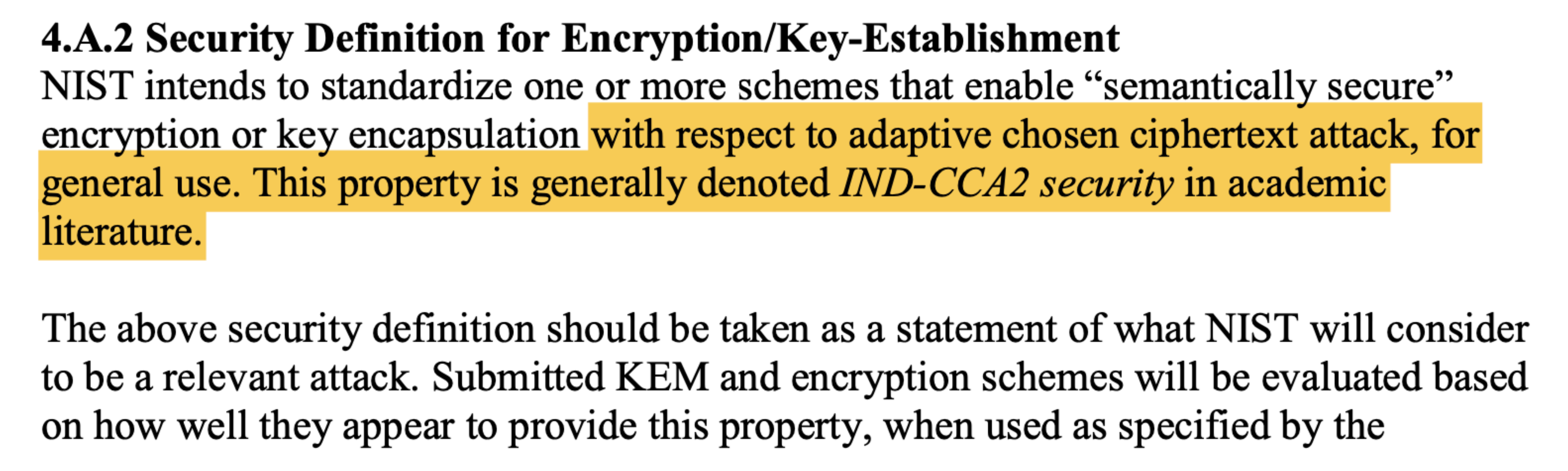
1980s: Formal definitions, constructions and security proofs

Shafi
Goldwasser

Silvio
Micali

# A BRIEF HISTORY OF MODERN CRYPTOGRAPHY

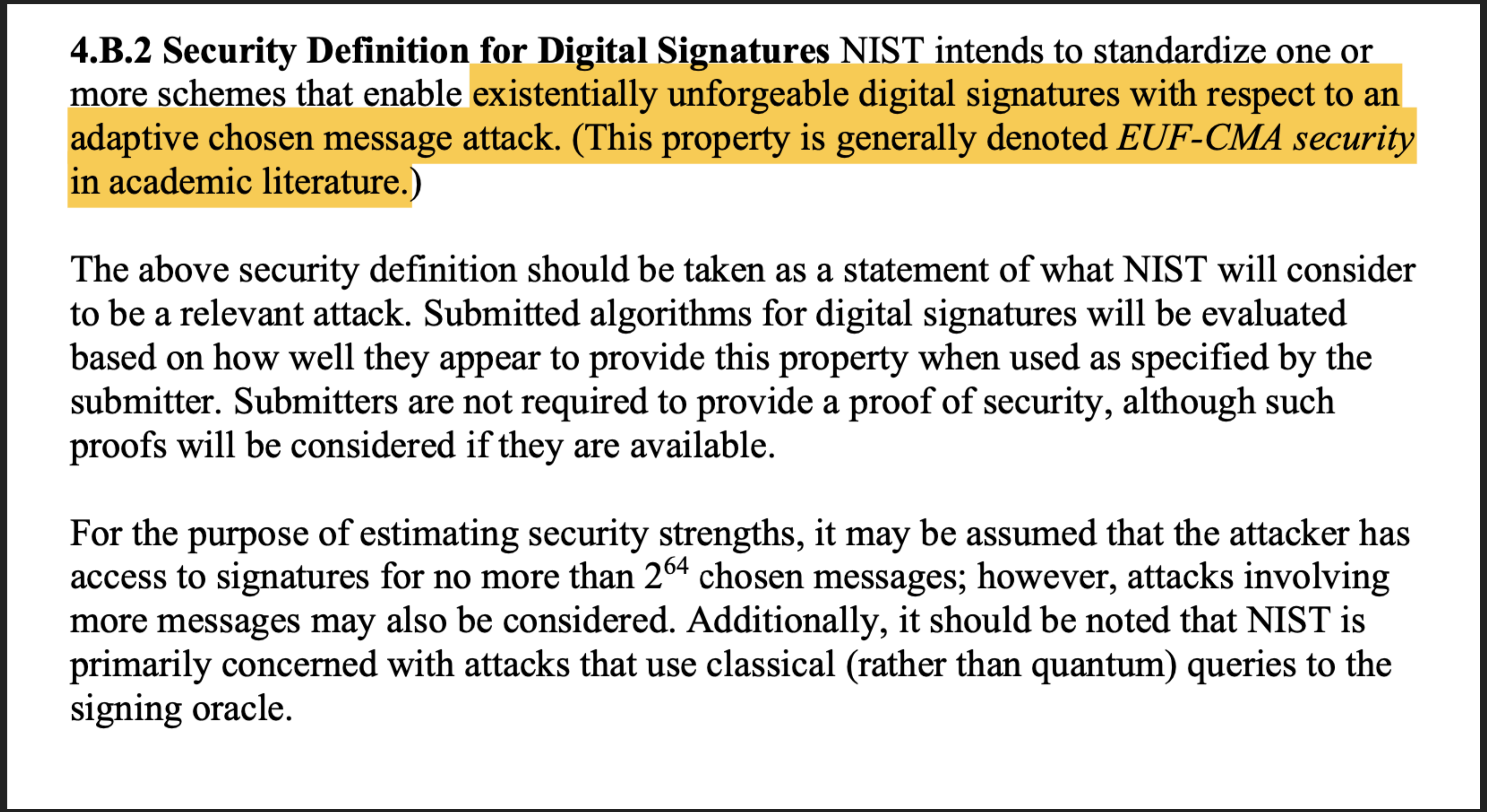
Today



**4.A.2 Security Definition for Encryption/Key-Establishment**
NIST intends to standardize one or more schemes that enable "semantically secure" encryption or key encapsulation with respect to adaptive chosen ciphertext attack, for general use. This property is generally denoted *IND-CCA2 security* in academic literature.

The above security definition should be taken as a statement of what NIST will consider to be a relevant attack. Submitted KEM and encryption schemes will be evaluated based on how well they appear to provide this property, when used as specified by the

NIST call for post-quantum encryption



**4.B.2 Security Definition for Digital Signatures** NIST intends to standardize one or more schemes that enable existentially unforgeable digital signatures with respect to an adaptive chosen message attack. (This property is generally denoted *EUF-CMA security* in academic literature.)

The above security definition should be taken as a statement of what NIST will consider to be a relevant attack. Submitted algorithms for digital signatures will be evaluated based on how well they appear to provide this property when used as specified by the submitter. Submitters are not required to provide a proof of security, although such proofs will be considered if they are available.

For the purpose of estimating security strengths, it may be assumed that the attacker has access to signatures for no more than $2^{64}$ chosen messages; however, attacks involving more messages may also be considered. Additionally, it should be noted that NIST is primarily concerned with attacks that use classical (rather than quantum) queries to the signing oracle.

NIST call for post-quantum signatures

We will see these definitions over the next few lectures …

# COURSE OUTLINE

# LECTURE 1

Intro to private key encryption;

# LECTURE 2

Private key enc. construction; attack on PKCS v1.5 enc. standard

# LECTURE 3

Intro to message authentication codes; construction

# LECTURE 4

Fixing PKCS v1.5 enc. using message auth. codes

# LECTURE 5

Intro to public key encryption; construction

# LECTURE 6

Intro to digital signatures; construction

# LECTURE 1

## PART 1: PRIVATE KEY ENCRYPTION – OUR FIRST SECURITY DEFINITION AND CONSTRUCTION

# TOY THREAT SCENARIO

King and admiral share secret info. beforehand

Later, King wants to send exactly one message

Admiral should learn the message

No one else should learn anything

# SYNTAX FOR PRIVATE KEY ENCRYPTION

Key space $\mathcal{K}$ Msg. space $\mathcal{M}$

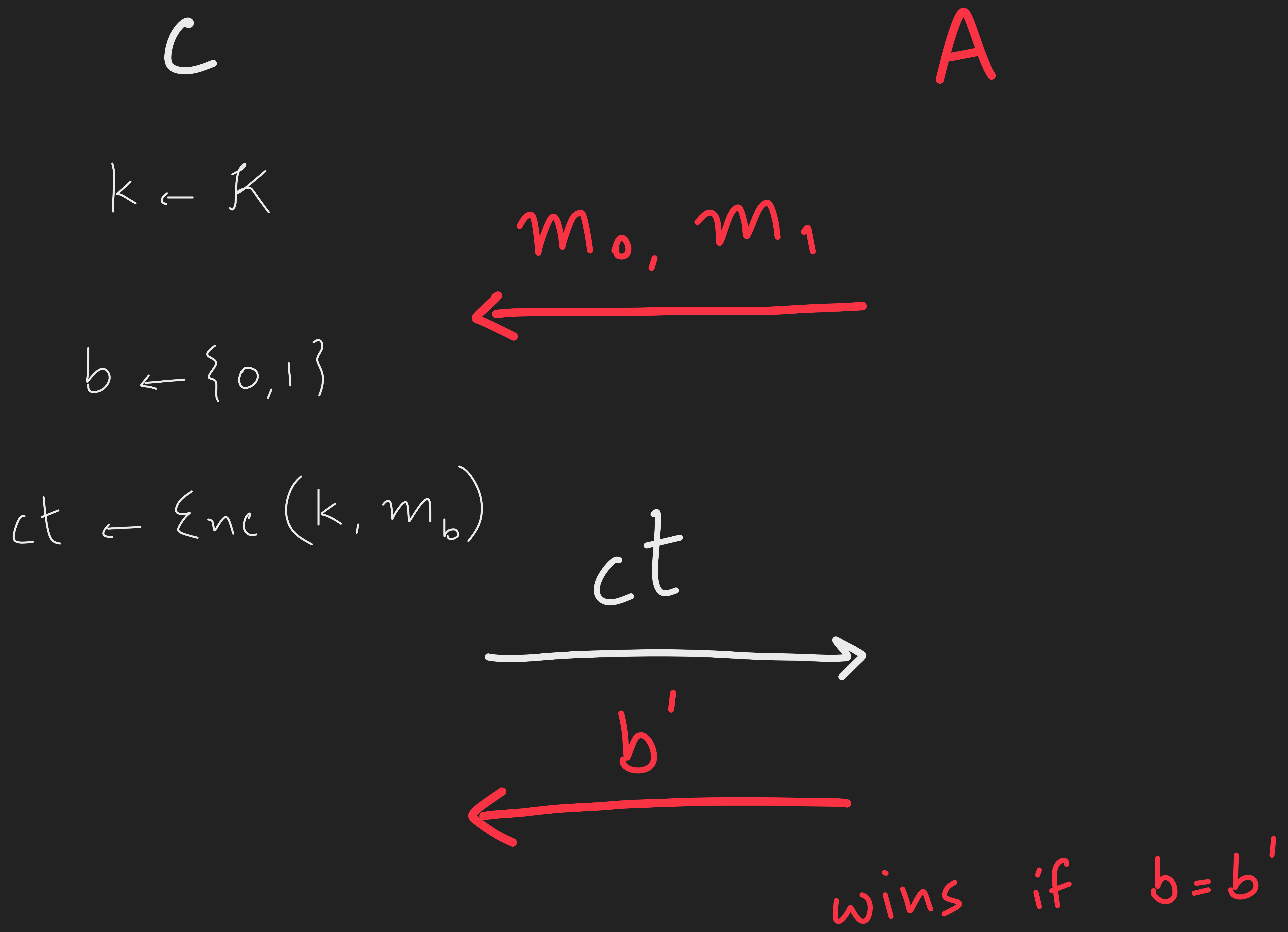
Ciphertext sp. $\mathcal{C}$

$$\text{Enc}(\overset{\nearrow \mathcal{K}}{\text{key}}, \overset{\nearrow \mathcal{M}}{\text{msg}}) \longrightarrow \text{ct} \nearrow \mathcal{C}$$

$$\text{Dec}(\text{key}, \text{ct}) \longrightarrow \text{msg}$$

$$\forall k, m \quad \text{Dec}(k, \text{Enc}(k, m)) = m$$

# FORMAL SECURITY DEFINITION FOR TOY THREAT SCENARIO



C

A

$k \leftarrow \mathcal{K}$

$m_0, m_1$

$b \leftarrow \{0,1\}$

$ct \leftarrow Enc(k, m_b)$

$ct$

$b'$

wins if $b = b'$

$(Enc, Dec)$ is

ONE-TIME

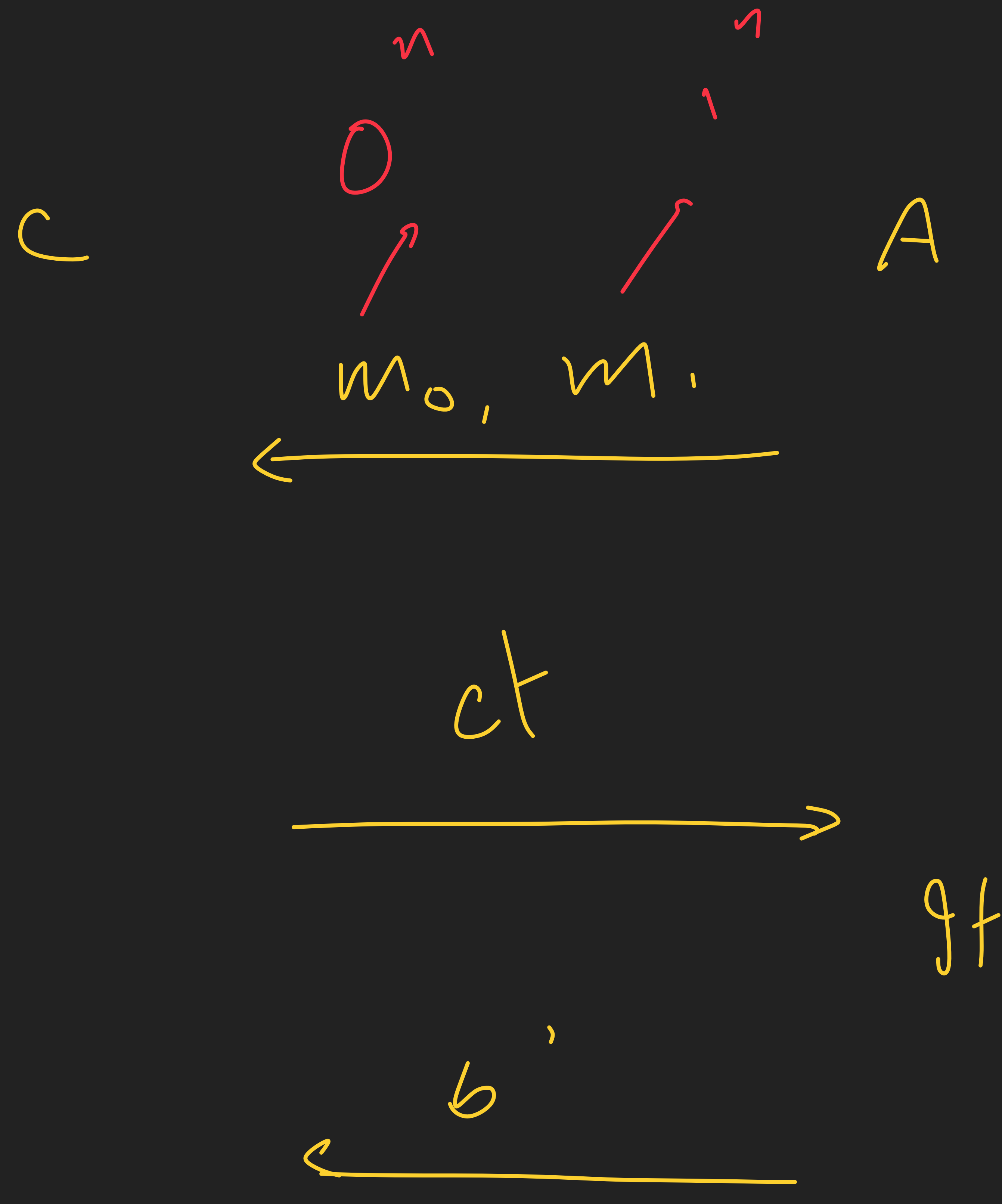
PERFECTLY SECURE

if $\forall A$,

$\Pr[A \text{ wins}] = 1/2$

$$\left.\begin{aligned} \mathrm{Enc}(k, m) &= m \\ \mathrm{Dec}(k, ct) &= ct \end{aligned}\right]$$

Does this satisfy our def?



If $ct = b^n$ send $b$.

A wins w.p. 1.

# SHANNON'S ENCRYPTION SCHEME

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

bitwise XOR

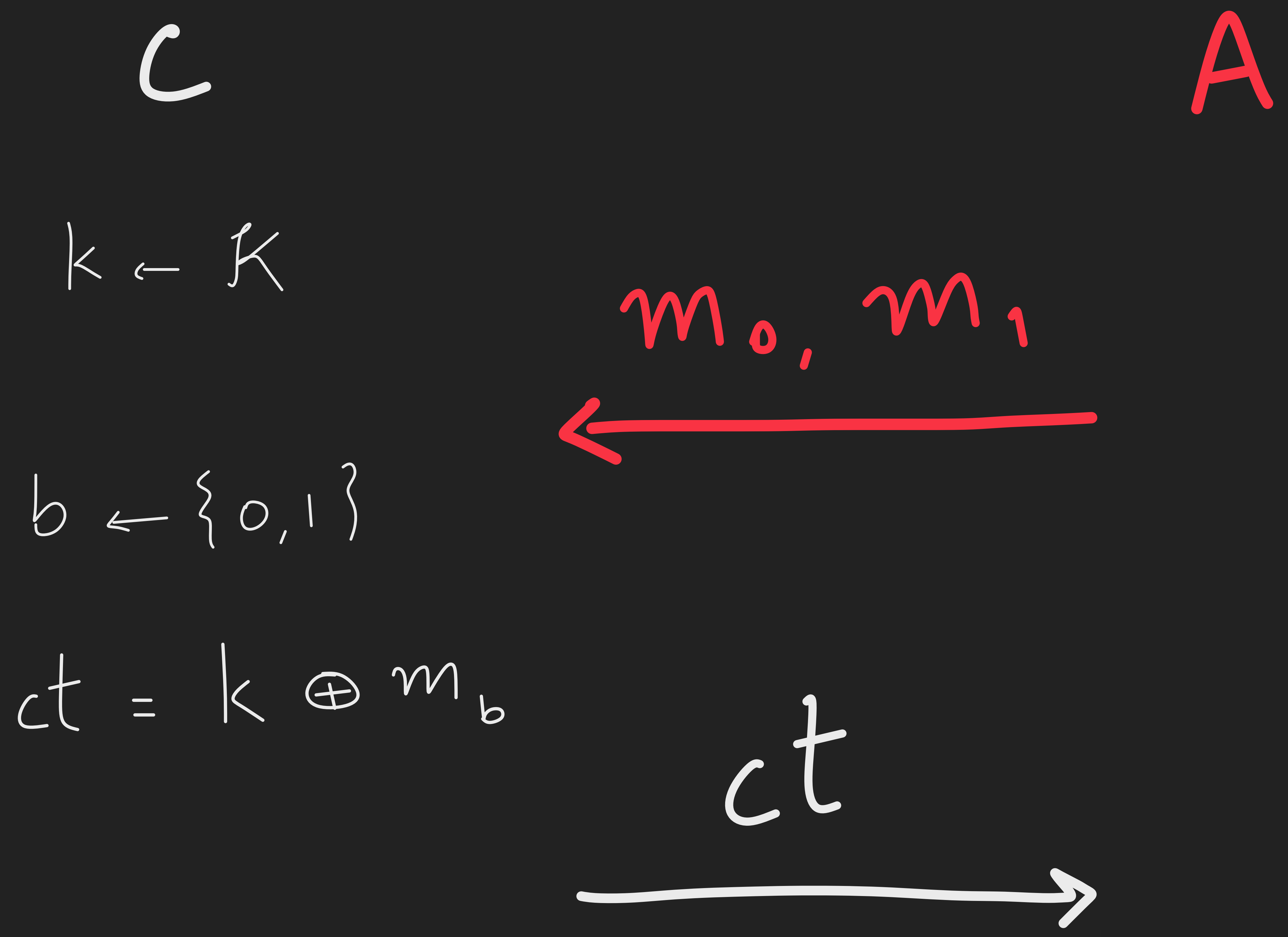
$$Enc(k, m) = k \oplus m$$

$$Dec(k, ct) = k \oplus ct$$

$$\forall k, m, \quad Dec(k, Enc(k, m)) = k \oplus k \oplus m$$

$$= m$$

# SHANNON'S ENCRYPTION SCHEME IS ONE-TIME SECURE



$k \leftarrow \mathcal{K}$

$b \leftarrow \{0,1\}$

$ct = k \oplus m_b$

# ANY OTHER ONE-TIME SECURE CANDIDATES?

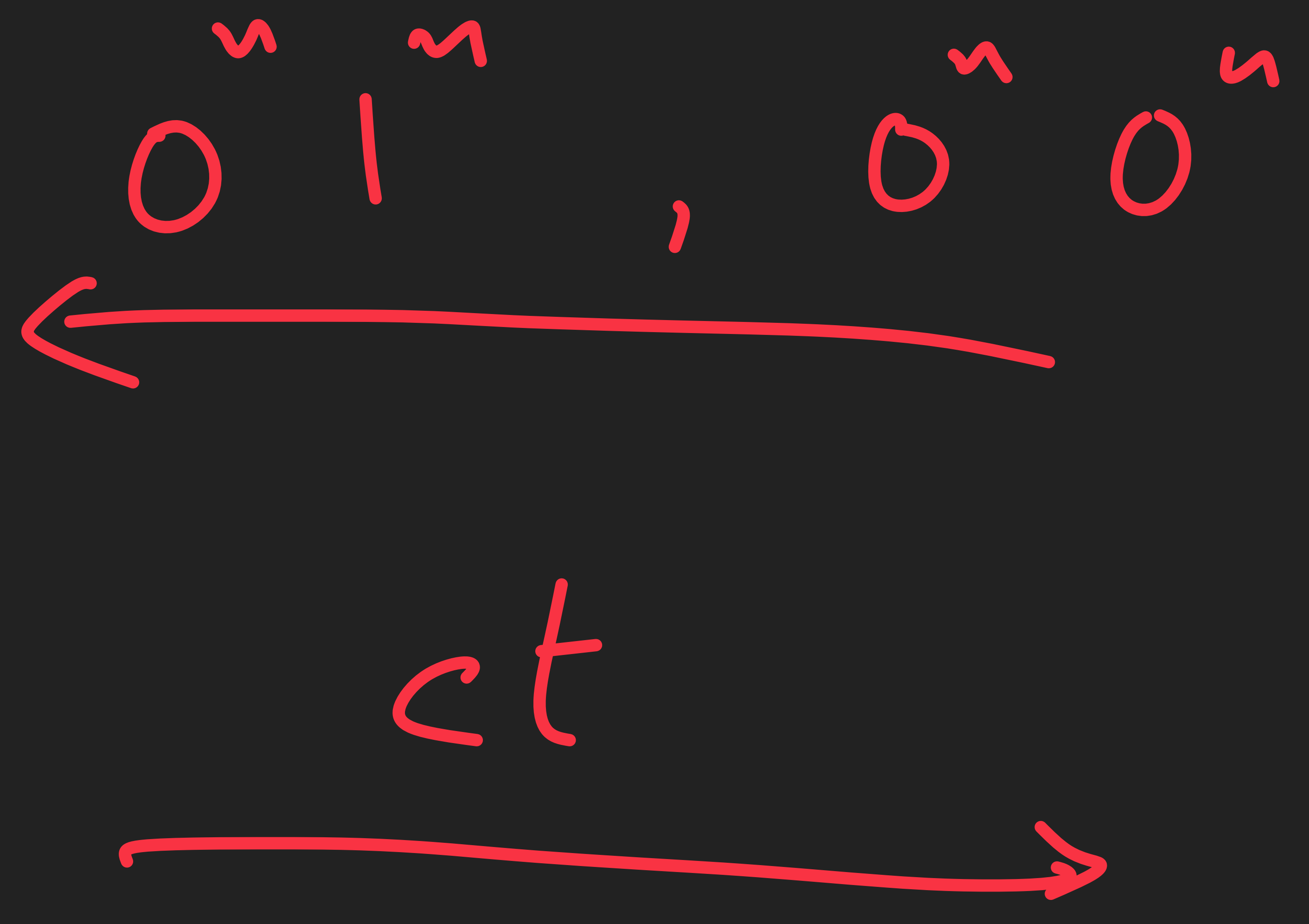
$\mathcal{K} = \{0,1\}^n$ $\mathcal{M} = \{0,1\}^{2n}$

Not secure

$\mathrm{Enc}(k, m)$ :

$$\tilde{k} = k \| k$$

$$ct = \tilde{k} \oplus m$$



If first half and second half of ct are same, then send 1.

# ONE-TIME SCHEMES ARE QUITE IMPRACTICAL

Need a different key for every message

PROJECT VENONA

One-time **perfectly secure** schemes have other limitations :

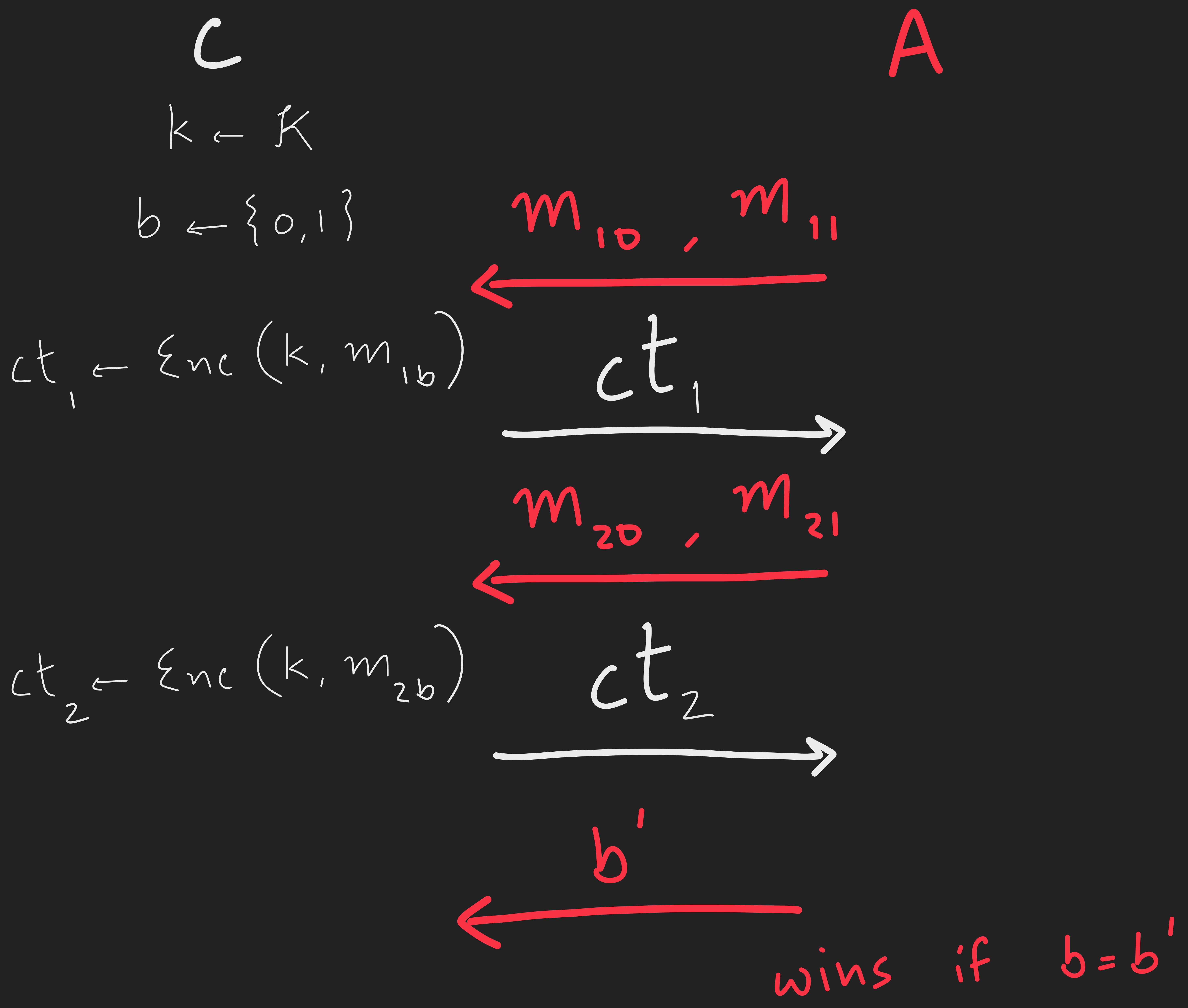
size of message space bounded

(Shannon’s Theorem - see Assignment 1)

# LECTURE 1

## PART 2: GOING BEYOND ONE-TIME SECURITY

# DEFINING TWO-TIME PERFECT SECURITY



$C$

$A$

$k \leftarrow \mathcal{K}$

$b \leftarrow \{0,1\}$

$m_{10}, m_{11}$

$ct_1 \leftarrow \mathcal{E}nc(k, m_{1b})$

$ct_1$

$m_{20}, m_{21}$

$ct_2 \leftarrow \mathcal{E}nc(k, m_{2b})$

$ct_2$

$b'$

wins if $b = b'$

$(\mathcal{E}nc, Dec)$ is

TWO-TIME

PERFECTLY SECURE

if $\forall A$,

$$\Pr[A \text{ wins}] = 1/2$$

# CAN ANY ENCRYPTION SCHEME BE TWO-TIME PERFECTLY SECURE?

Det. Enc : not possible

$$\xleftarrow{0^n,\ 1^n}$$

$$\xrightarrow{ct_1}$$

$$\xleftarrow{0^n,\ z \neq 1^n}$$

$$\xrightarrow{ct_2}$$

if $ct_1 = ct_2$

Qn : If enc. is randomized. can we achieve two time perfect sec.?