COL759:
CRYPTOGRAPHY AND COMPUTER SECURITY

2022-23 (SEMESTER 1)

LECTURE 1: INTRO

COL759 IS NOT ABOUT …

Computer Security
(SIL 765)

(COV 885)

Symmetric Key Encryption

Message Authentication Codes

Collision resistant
hash functions

Authenticated Encryption

Public Key Encryption

Signatures

Zero Knowledge Proofs

COL759

COL759 IS ABOUT …

Formal security definitions, and security proofs

THEORETICAL COURSE

COURSE OBJECTIVES

- Develop ‘crypto mindset’

- Modelling threats via security definitions

- Learn the ‘atomic’ building blocks of crypto, and how they’re used for building more complex primitives

- Understand how to prove security

COL759 IS ABOUT . . .

4-STEP RECIPE FOR A CRYPTO PRIMITIVE

1. Define security for the primitive
2. Figure out the required building blocks
3. Propose construction
4. Prove construction satisfies security definition

ANALOGY:
LEGO BLOCKS

THE LEGO ANALOGY

Atomic building blocks

Our desired crypto primitive

THE LEGO ANALOGY

LEGO

Lego blocks are immutable.

Can't manufacture your own Lego blocks

CRYPTO

DO NOT modify the building blocks

DO NOT implement the building blocks
(use existing libraries)

WHY FORMAL DEFINITIONS AND PROOFS OF SECURITY?

SYMMETRIC KEY ENCRYPTION

Key Space $\mathscr{K}$

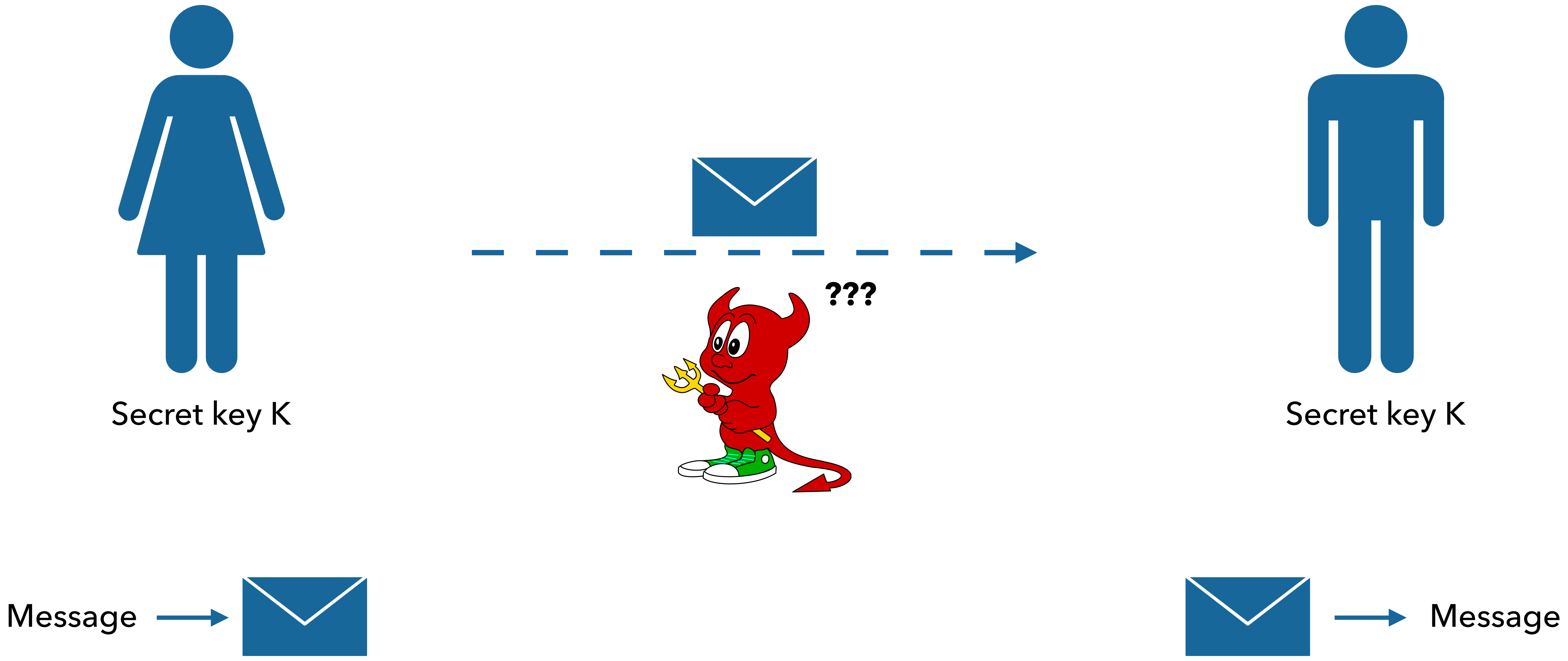
$$\text{Encrypt}(\text{mesage}, \text{secret key}) \to \text{ciphertext}$$

$$\text{Decrypt}(\text{ciphertext}, \text{secret key}) \to \text{message}/\perp$$

CORRECTNESS

$$\text{Decrypt}(\text{Encrypt}(\text{m}, \text{k}), \text{k}) = \text{m}$$

SYMMETRIC KEY ENCRYPTION



A BRIEF HISTORY OF ENCRYPTION SCHEMES

1. Caesar's cipher

- **Secret key:**
  Integer s
- **Encrypt:**
  shift each character forward by s positions

BROKEN CIPHER !!

Attack via brute force

2. Substitution cipher

- **Secret key:**
  Permutation over the alphabets
- **Encrypt:**
  substitute each character according to permutation in secret key

BROKEN CIPHER !!

Attack via frequency analysis

3. Vigenère's cipher

- **Secret key:**
  n different permutations

- **Encrypt:**
  For character at position i, use substitution with (i mod n)th permutation

le chiffrage indéchiffrable

(the indecipherable cipher)

3. Vigenère's cipher

- **Secret key:**
  n different permutations

- **Encrypt:**
  For character at position i, use substitution with (i mod n)th permutation

Efficient algo. for breaking substitution cipher

$\Downarrow$

Efficient algo. for breaking Vigenère cipher

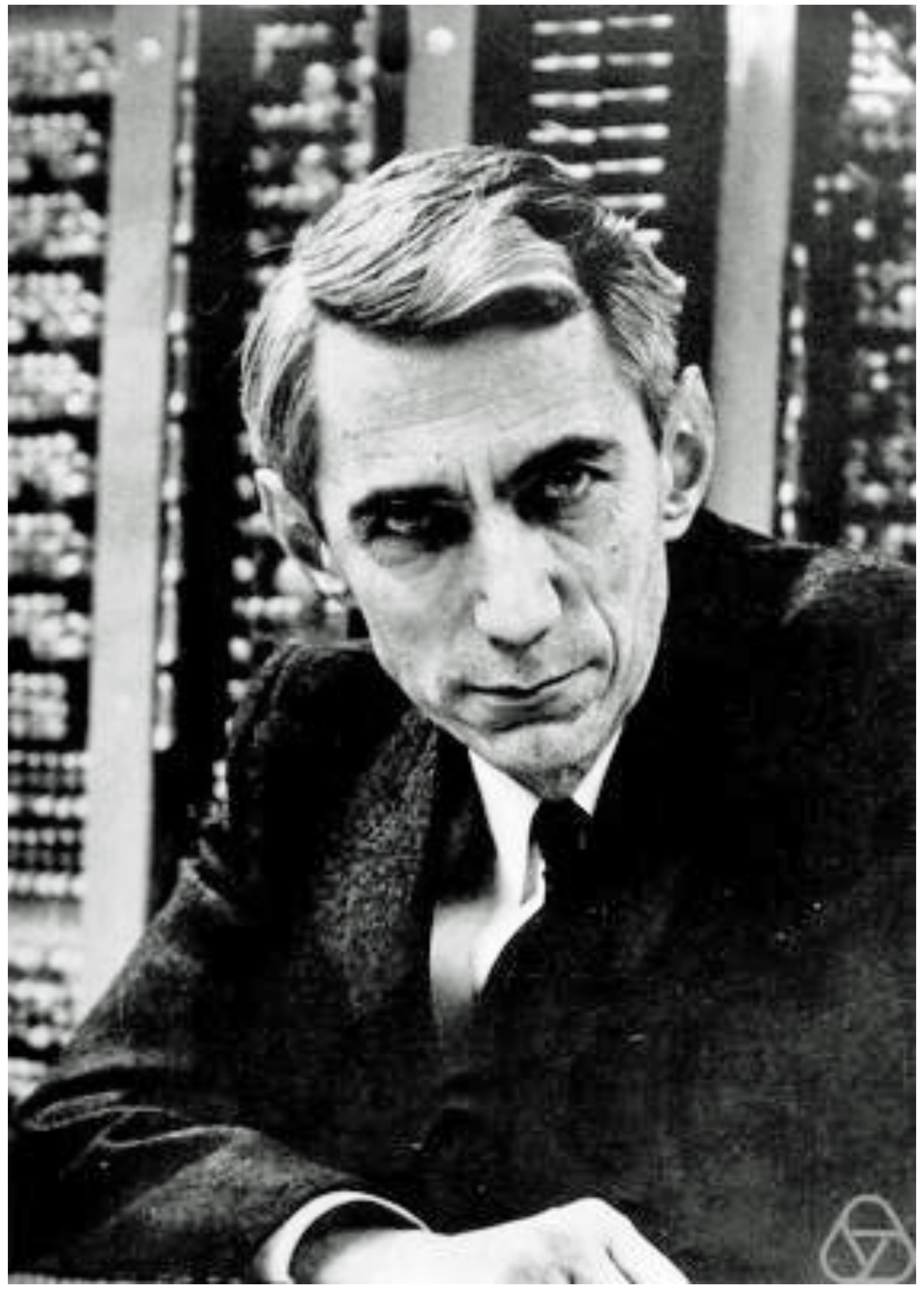
Is 'Double-Encrypt-Vigenere' secure?
What if n = length of message to be encrypted?

A BRIEF HISTORY OF ENCRYPTION SCHEMES

4. Rotor machines (Enigma)

BROKEN DURING WW-II

5. Shannon's One-Time Pad



"Communication Theory of Secrecy Systems"

(1945)

Perfectly secure encryption scheme

Key cannot be reused

Must be as large as the message

6. Data Encryption Standard (DES)

(1970s)

Key Space : $\{0,1\}^{56}$

DES : $\{0,1\}^{64} \times \{0,1\}^{56} \rightarrow \{0,1\}^{64}$

DES^{-1} : $\{0,1\}^{64} \times \{0,1\}^{56} \rightarrow \{0,1\}^{64}$

DES can 'encrypt' 64 bit messages.
How to encrypt longer messages?

ATTACKS

Exhaustive search for key: ~ 2^{56} steps
Best known attack: ~ 2^{44} steps

Feasible using modern supercomputers

Can we extend key space appropriately?

6.1. Double DES (2DES)

Key Space : $\{0,1\}^{112}$

$$2DES\Big(m, (k_1, k_2)\Big) = DES\ \Big(DES(m, k_1), k_2\Big)$$

$$2DES^{-1}\Big(ct, (k_1, k_2)\Big) = DES^{-1}\ \Big(DES^{-1}(ct, k_2), k_1\Big)$$

ATTACKS

Previous attacks infeasible.

But a different (very simple) attack breaks 2DES

Triple DES (3DES) ?

7. Advanced Encryption Standard (AES)

(1990s)

Key Space : $\{0,1\}^{128}$

AES : $\{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$

AES^{-1} : $\{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$

AES can 'encrypt' 128 bit messages.
How to encrypt longer messages?

ATTACKS

Exhaustive search for key: ~ 2^{128} steps

Best known attack: ~ 2^{126} steps

Most widely used crypto algorithm

HARNESSING COMPUTATIONAL HARDNESS FOR CRYPTOGRAPHY

No efficient algo. for breaking AES

$\Downarrow$

Secure encryption scheme

CENTRAL THEME IN MODERN CRYPTO

Building blocks:
hard computational problems

Proof of security:
No efficient algo for problem

$\Downarrow$

Cryptosystem is secure

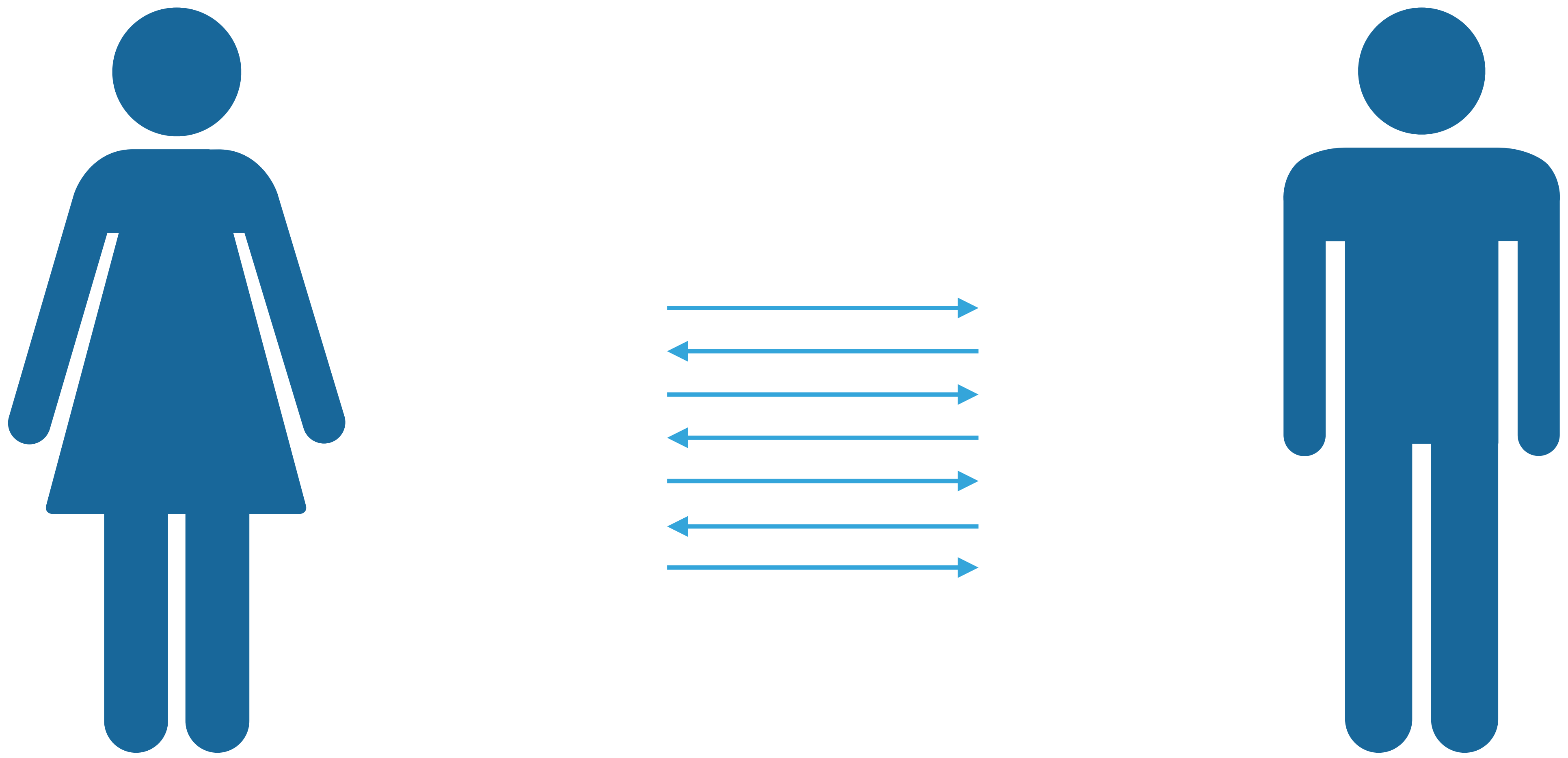
SOURCES OF HARD COMPUTATIONAL PROBLEMS

- Cryptographic standards: AES, SHA etc
- Number Theory
- Geometry
- Combinatorics …


COL759
CRYPTOGRAPHY

CRYPTO IS MAGIC !

Magic #1



x_0, x_1: strings

bit b

DESIDERATA

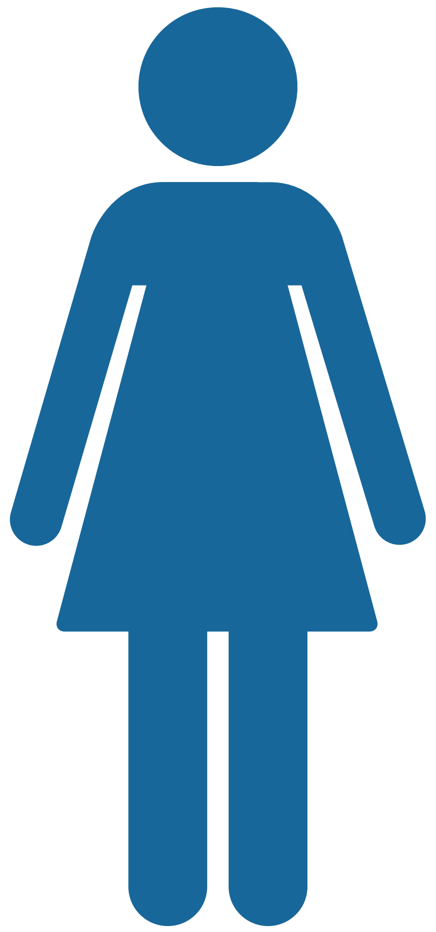
- Bob should learn x_b

- Alice should not learn b
  Bob should not learn x_{1-b}

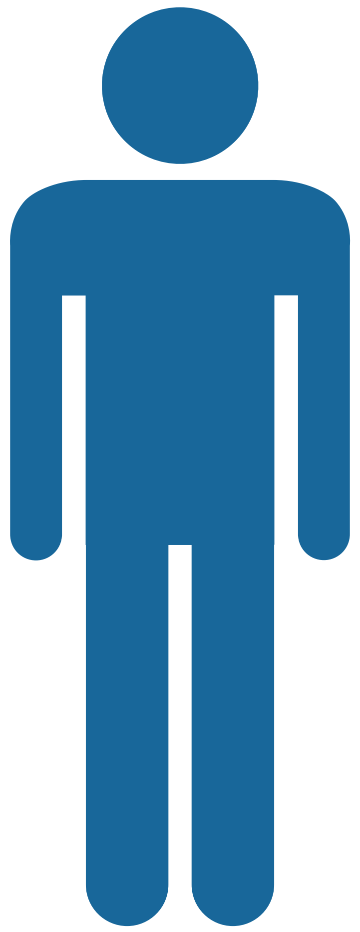
'Oblivious Transfer'

CRYPTO IS MAGIC !

Magic #2



x_0: string



x_1: string

DESIDERATA

- Alice and Bob should learn $f(x_0, x_1)$

- Alice should not learn x_1
  Bob should not learn x_0

'Multiparty Computation'

Magic #3

			7					
		2				3		
4				5	9		1	
			4				7	
	3			7	6	1		
6			8					
9				6	1		5	
					8			
	4							9

DESIDERATA

- Convince you that puzzle is solvable
- Without revealing any hint about solution

'Zero Knowledge Proofs'

COURSE INFO

Webpage: https://www.cse.iitd.ac.in/~koppula/courses/COL202_2102.html

Lecture notes on OneNote (_Content Library –> Lectures –> Lecture #)

COURSE POLICY

NON NEGOTIABLES

- Theoretical course: assignments and exams will involve writing formal security proofs
- Assignments: groups of size 1 or 2. Must be typed in Latex
- Strict plagiarism policy
- Please avoid using laptops/phone during the lecture

COURSE POLICY

NEGOTIABLES

- Grading: relative
  - Minor: 25%
  - Major: 30%
  - Assignments (4): 25%
  - Quizzes (best 5 of 6): 20%

Open-notes (handwritten notes only)
Longer duration for exams?

- Late Policy for assignments:
  - Three late days (cumulative)

- Please participate actively in class. Ask lots of questions
- Assignments : start early

THANK YOU!

(see you tomorrow)