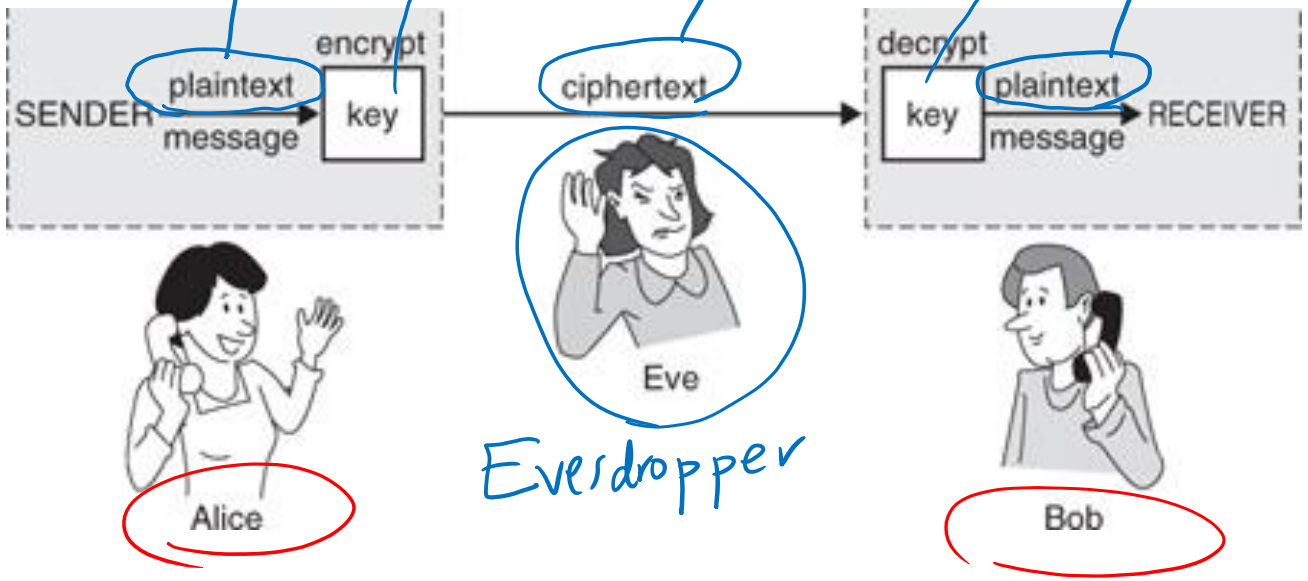
Special Topics in Cryptography

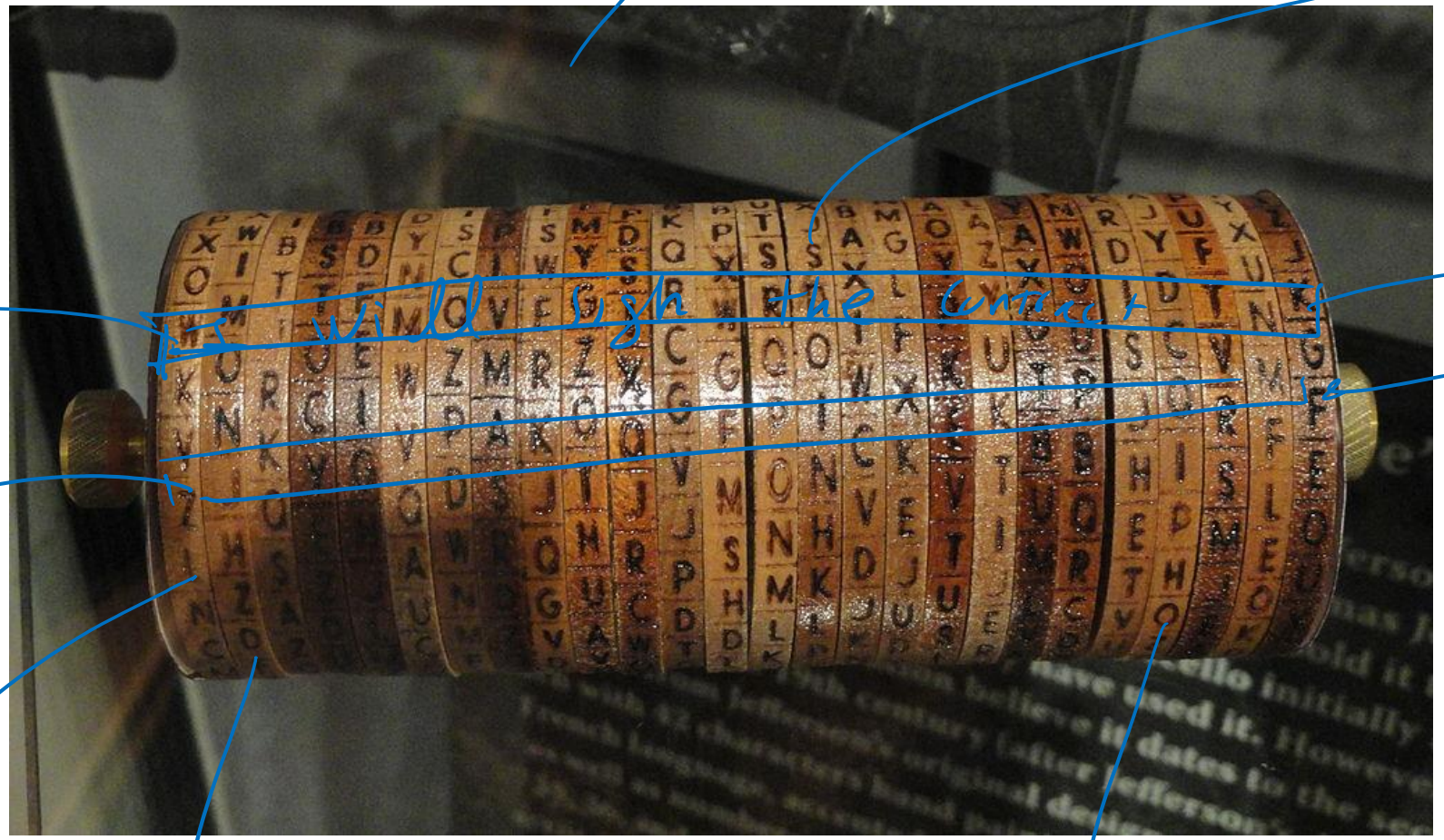
Mohammad Mahmoody

Cryptography’s main goals

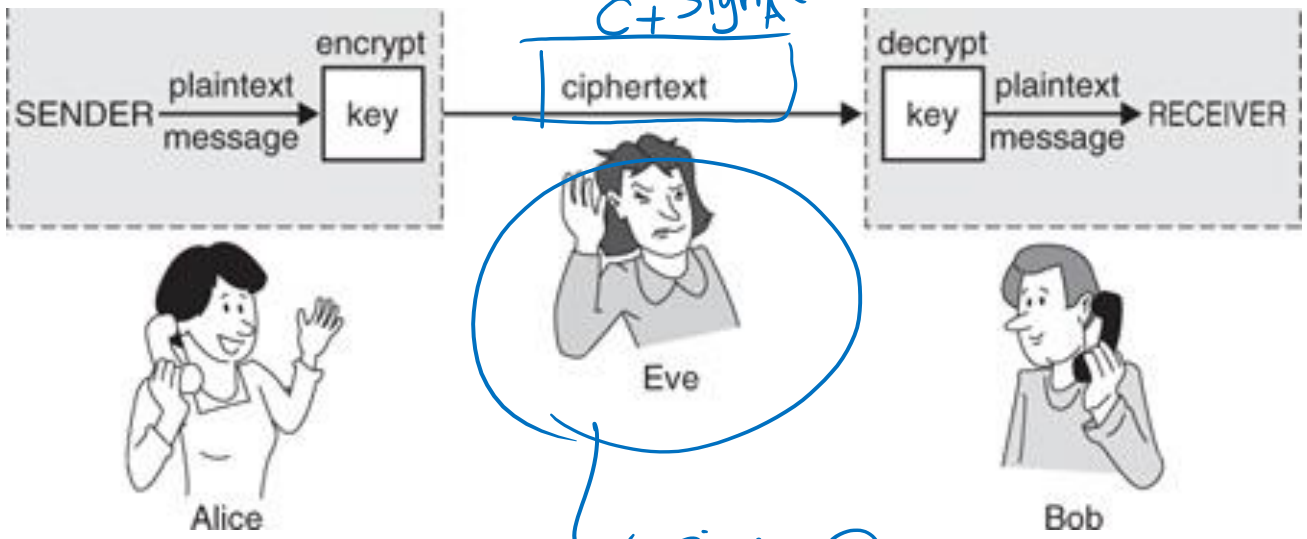
Secure communication



Historic Ciphers



Privacy / confidentiality



Violating Integrity of message.

Authentication

$C + Sign_A(C)$

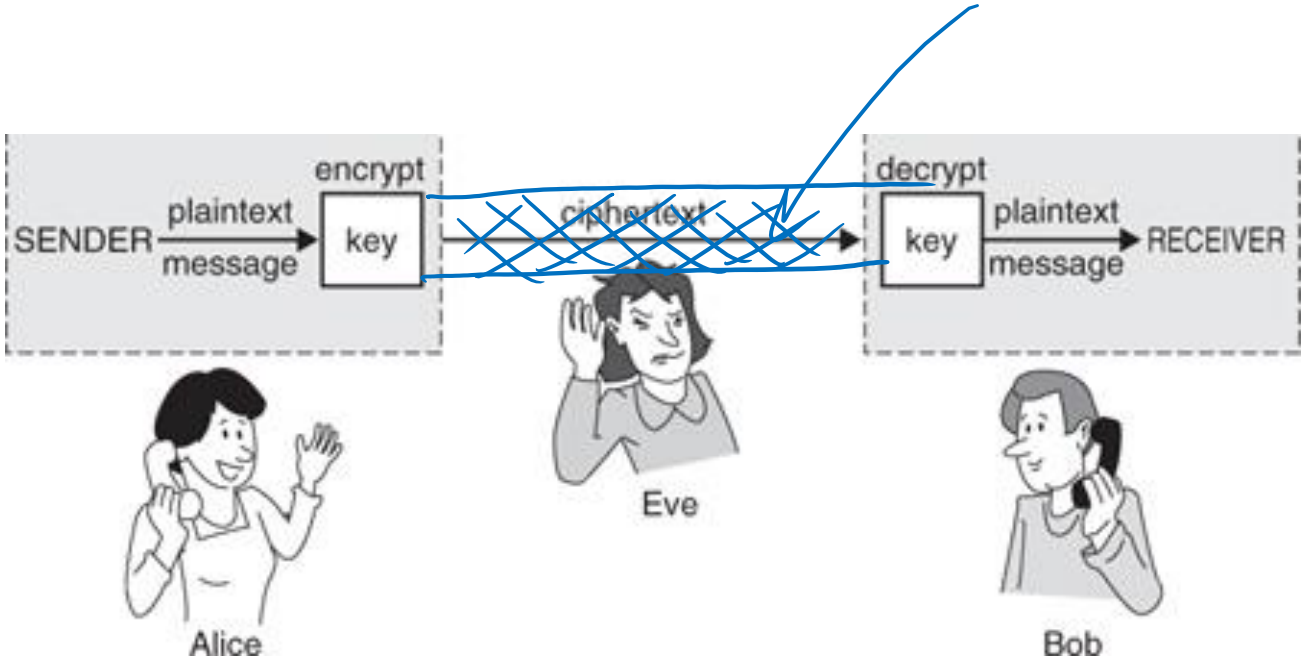
copies ©

we send c on behalf of Alice.

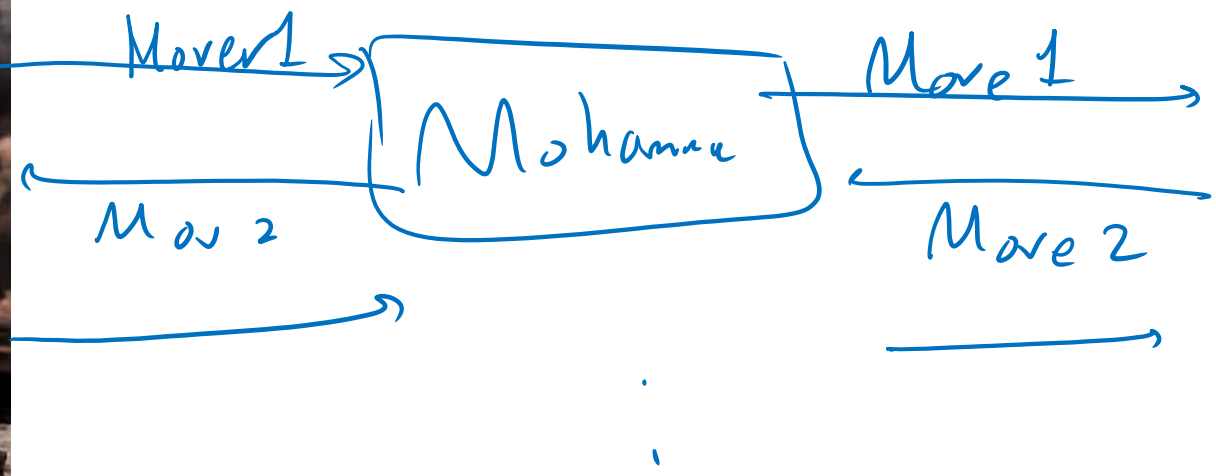
Integrity / Authentication

Privacy / Confidentiality
Integrity / Authentication

How to combine them.



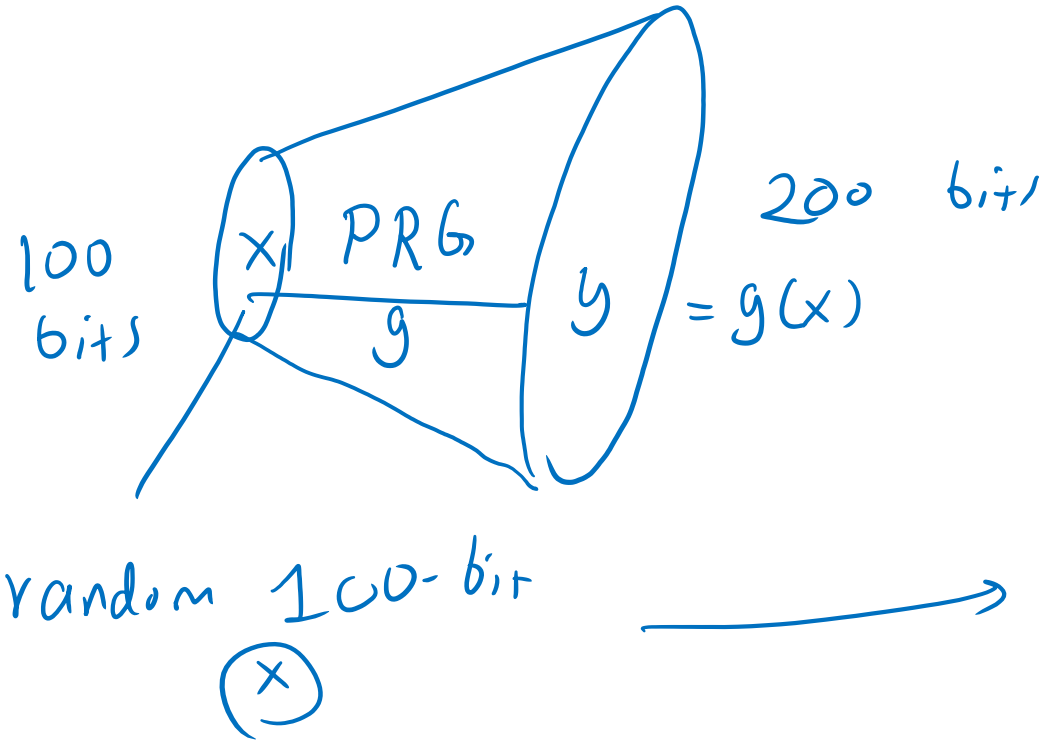
Not loosing in chess to the grand master

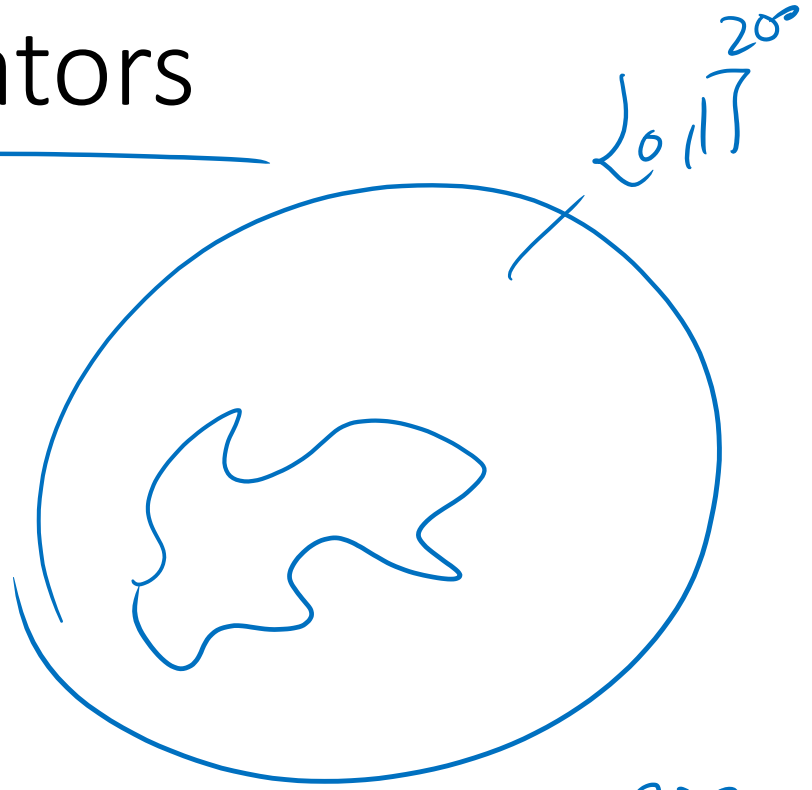


Tool:

Hash - Function

Pseudorandom ~~(number)~~ generators

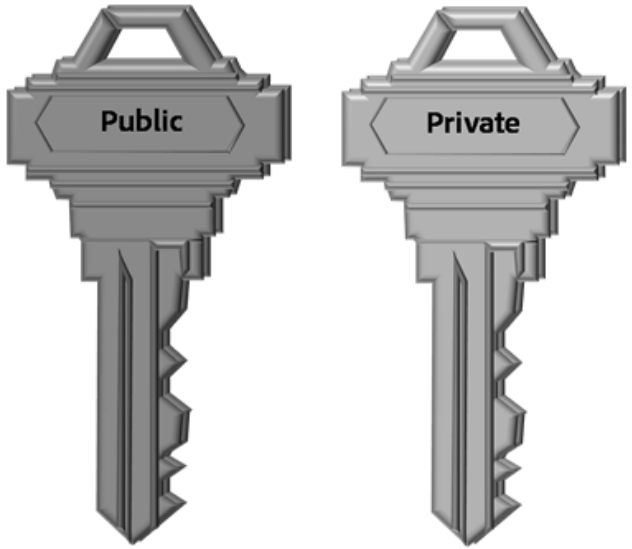


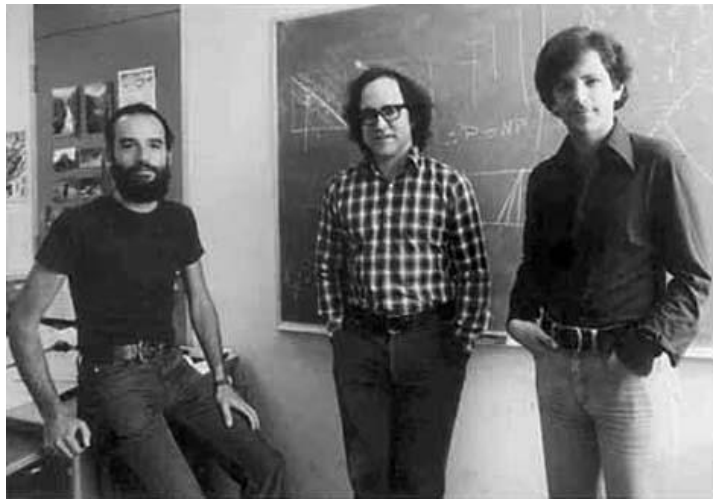


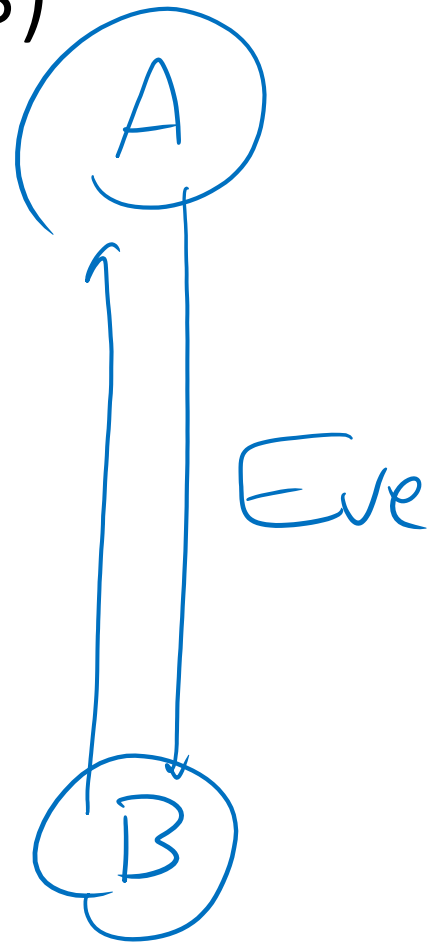
Look at $g(x) \in \{0,1\}^{200}$

Cryptography.

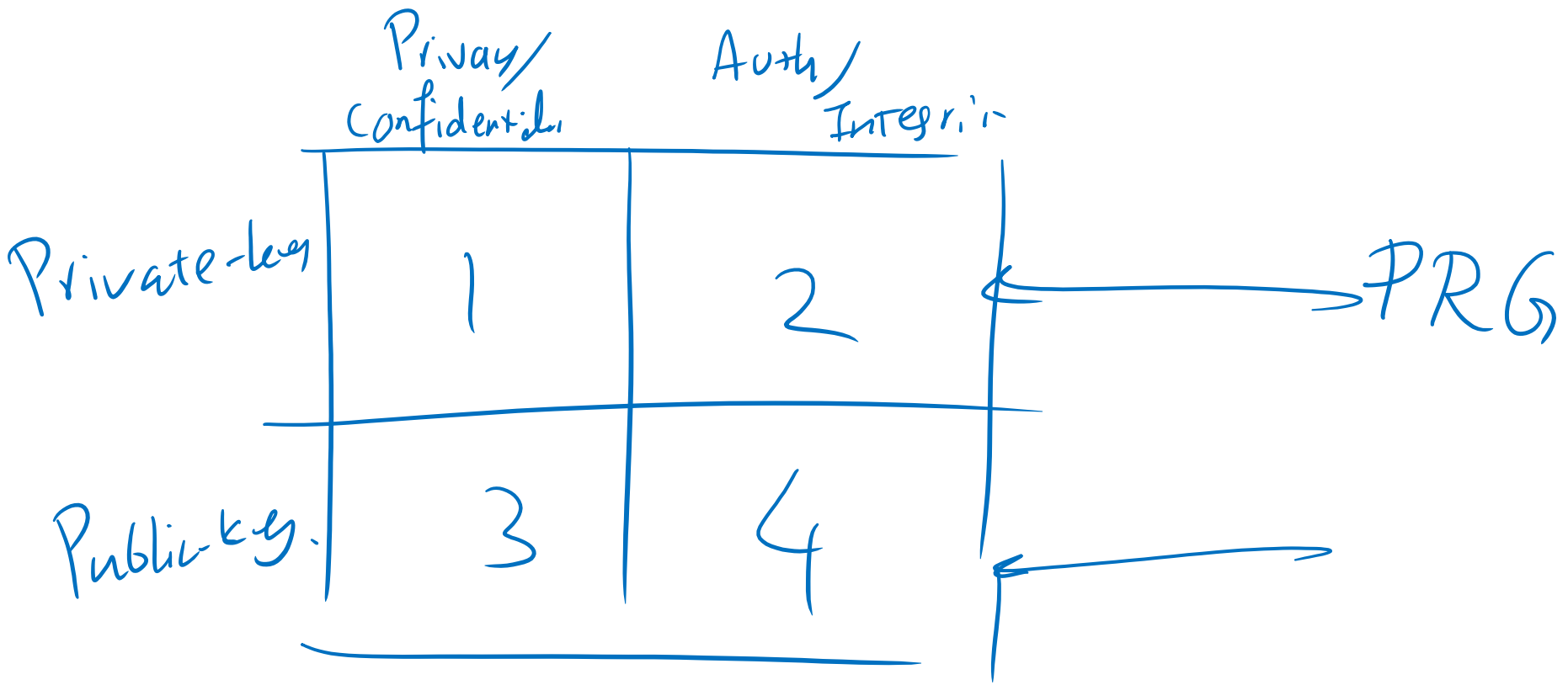
Public Key Encryption Revolution (70's)



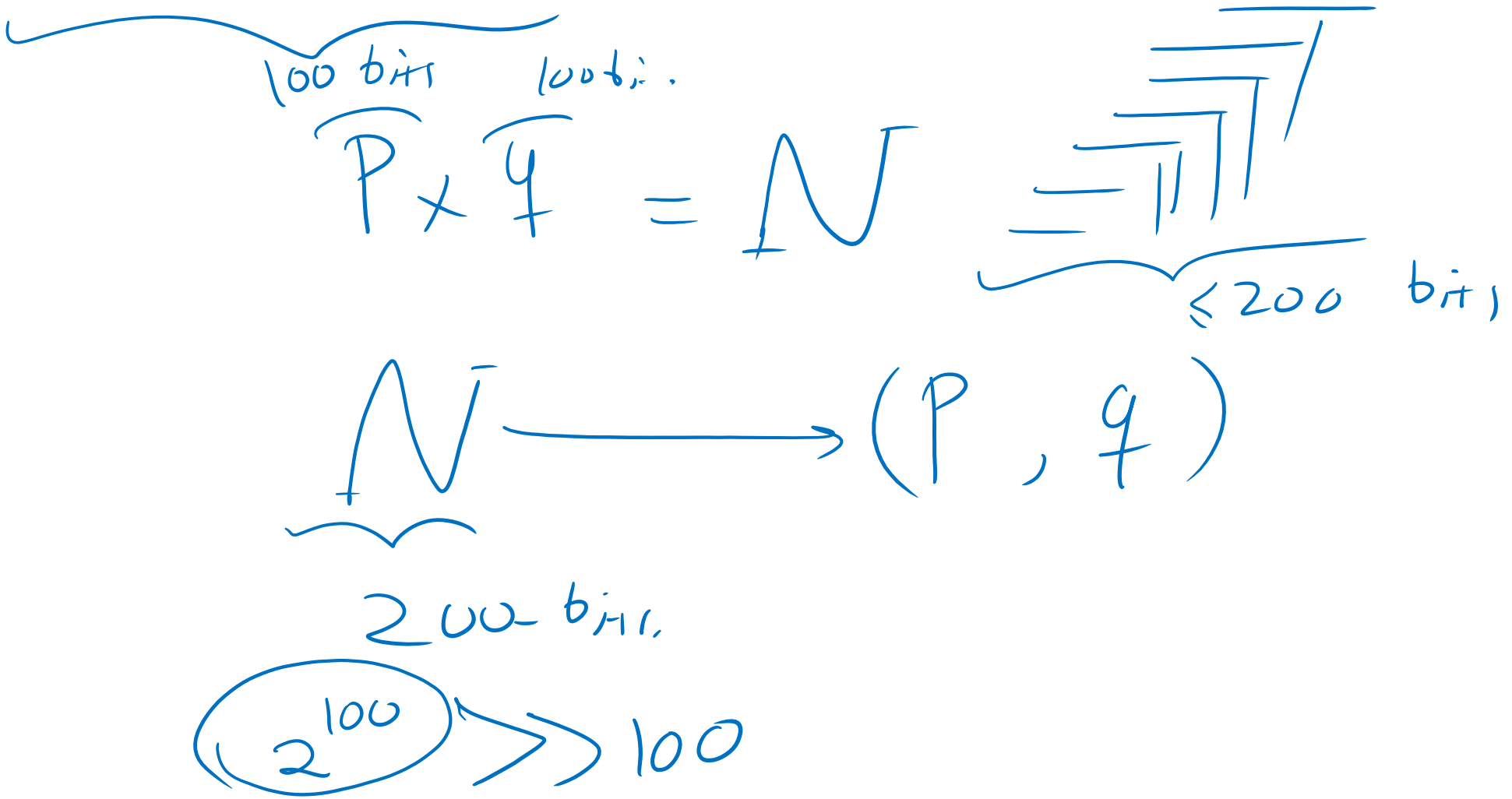




Four main problems in cryptographic



Main tool for public-key cryptography: Number theory and structured mathematics



Beyond Encryption and Authentication

Multi-party Computation

Yao's Billionaires Problem

x

$= \{l_1, \ldots, l_n\}$

$$f(x,y) \begin{cases} x > y : \boxed{-1} \\ x = y : \boxed{0} \\ x < y : \boxed{1} \end{cases}$$

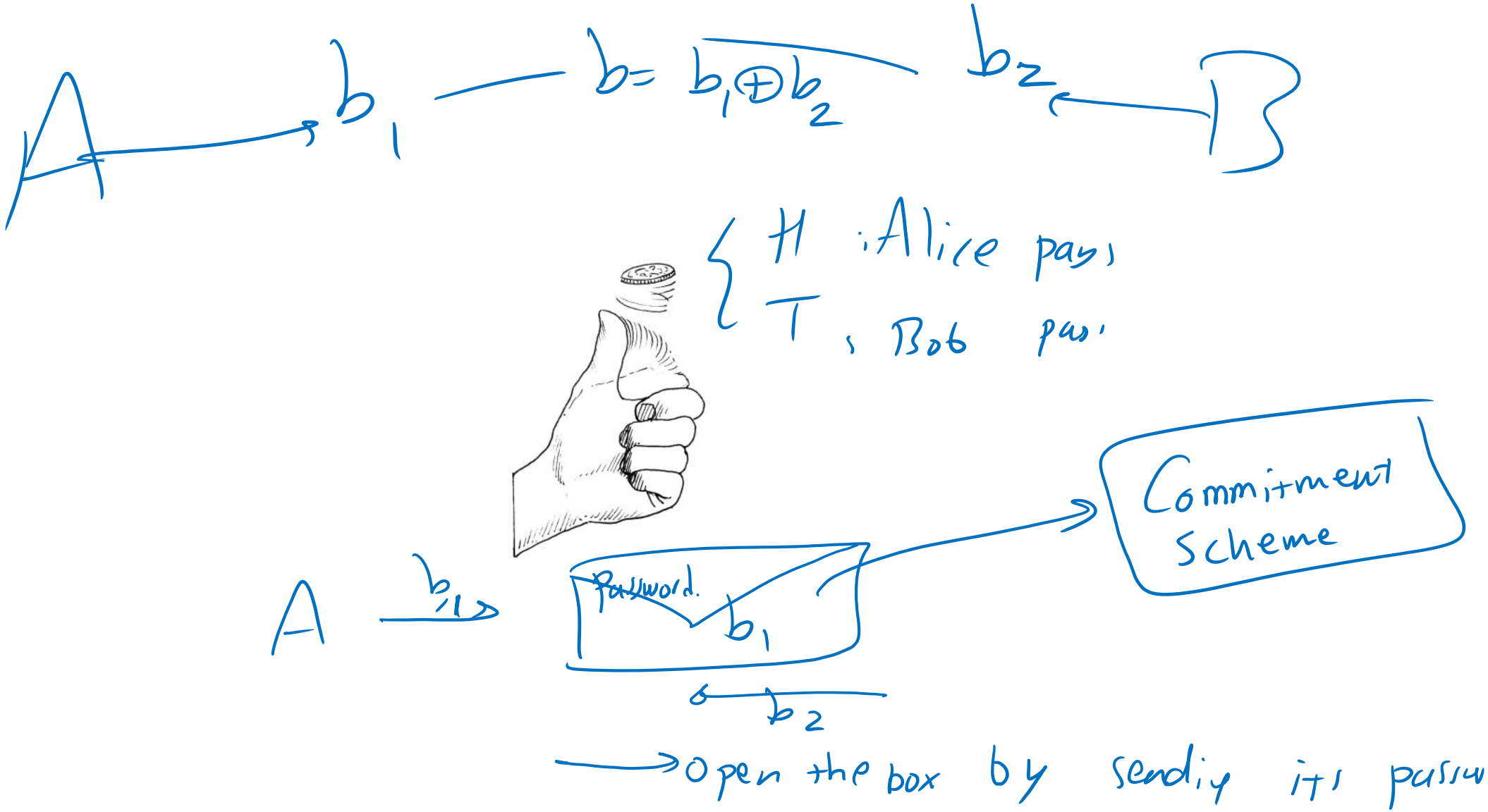
y

$\{l'_1, \ldots, l'_m\}$

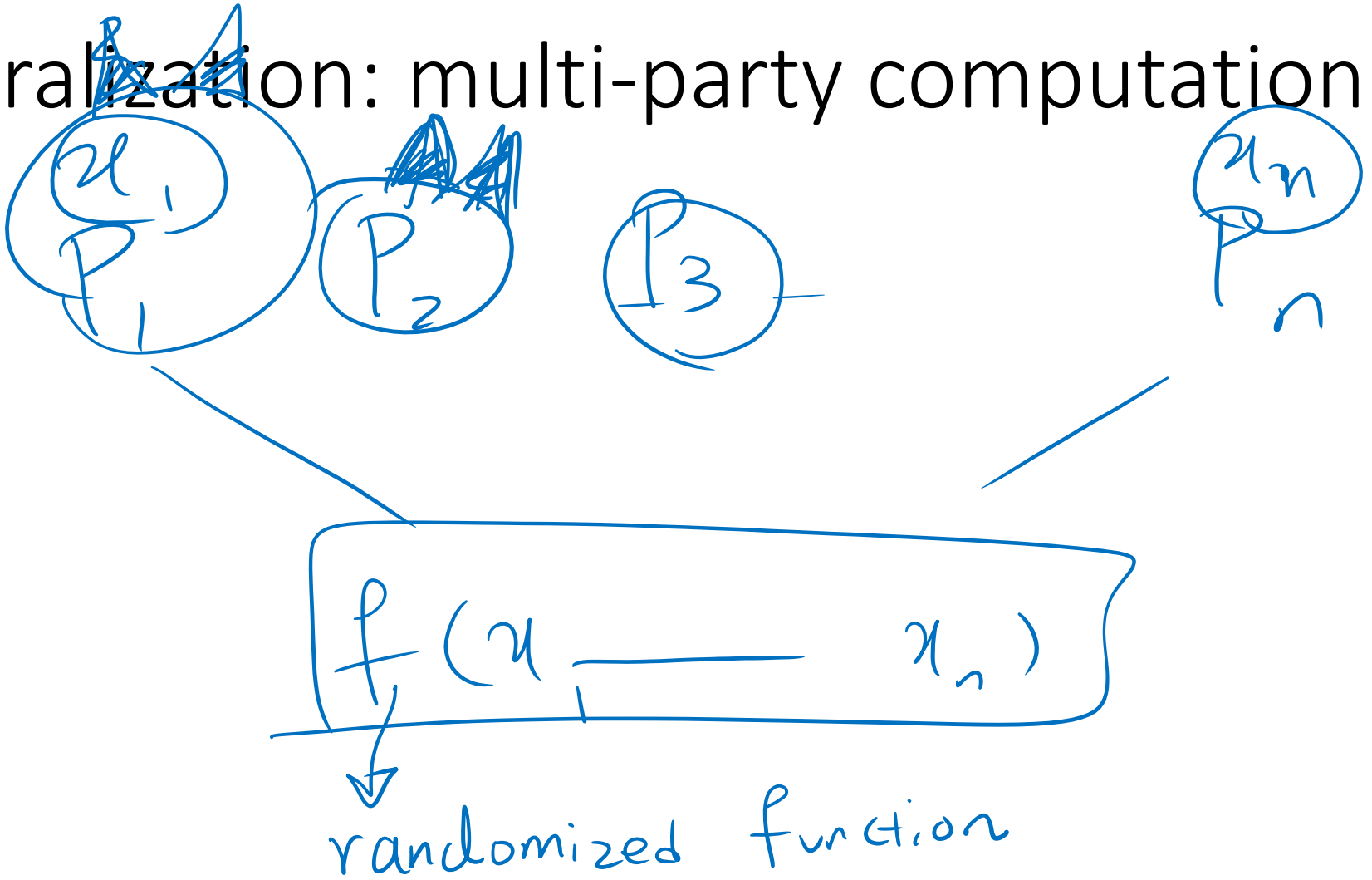
$f(x,y)$

$f(x,y) = \boxed{x \cap Y}$

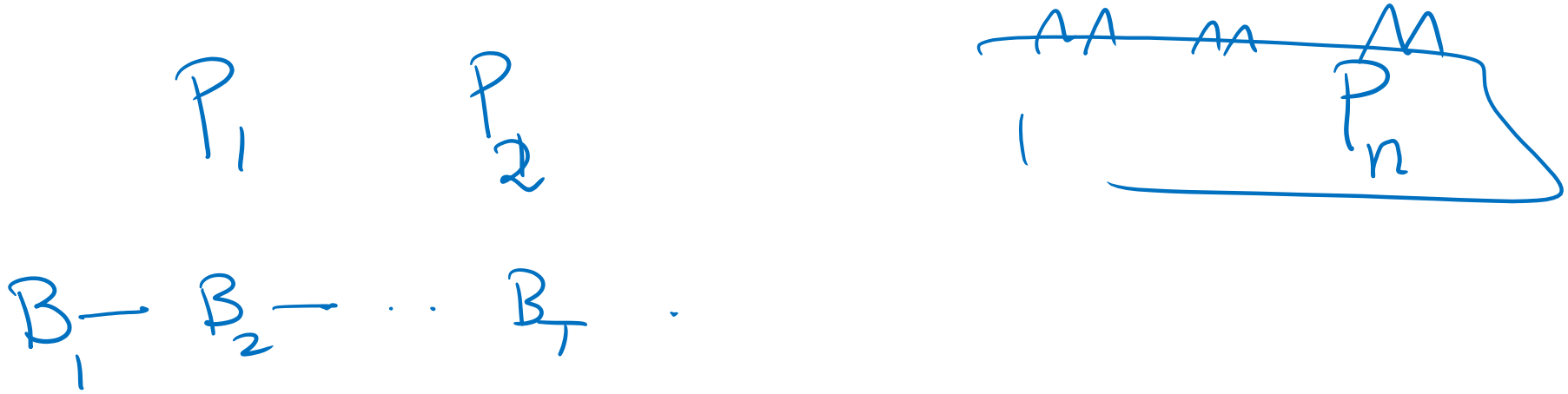
Poker over the phone



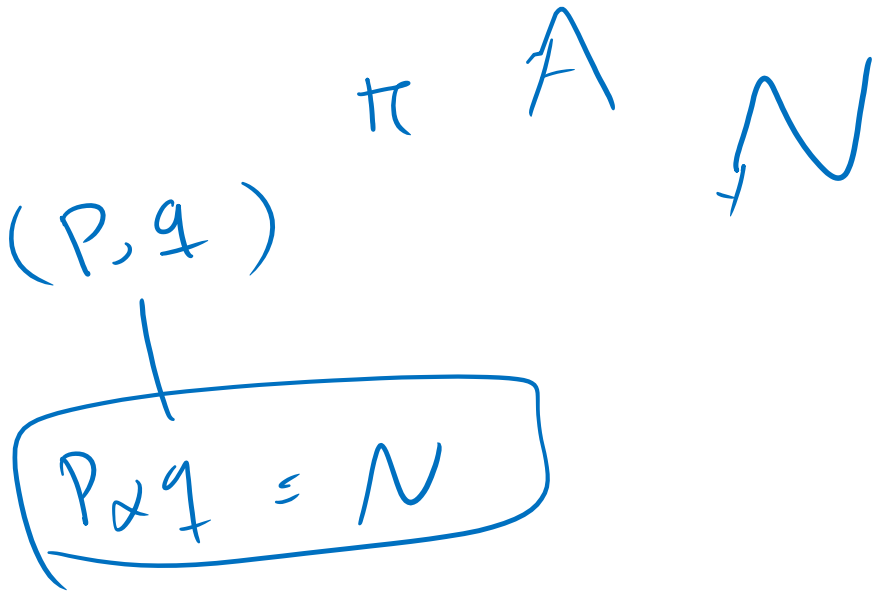
Generalization: multi-party computation



Multiparty consensus mechanisms (and block-chain protocols …)



Weird useful tool: Zero Knowledge Proofs



Goal:

Convince Bob that Alice "knows" P, q where P·q = N

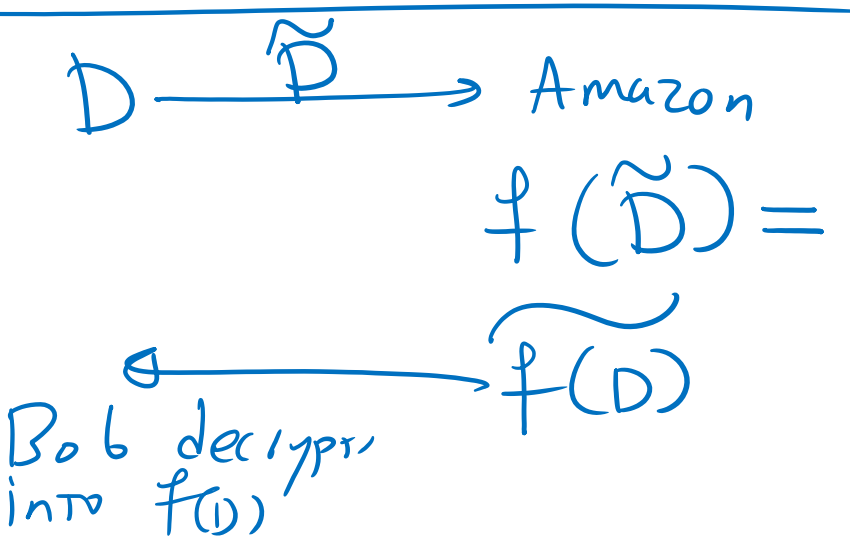
More powerful forms of Encryption

Homomorphic Encryption

Bob wants to do computation over data D.

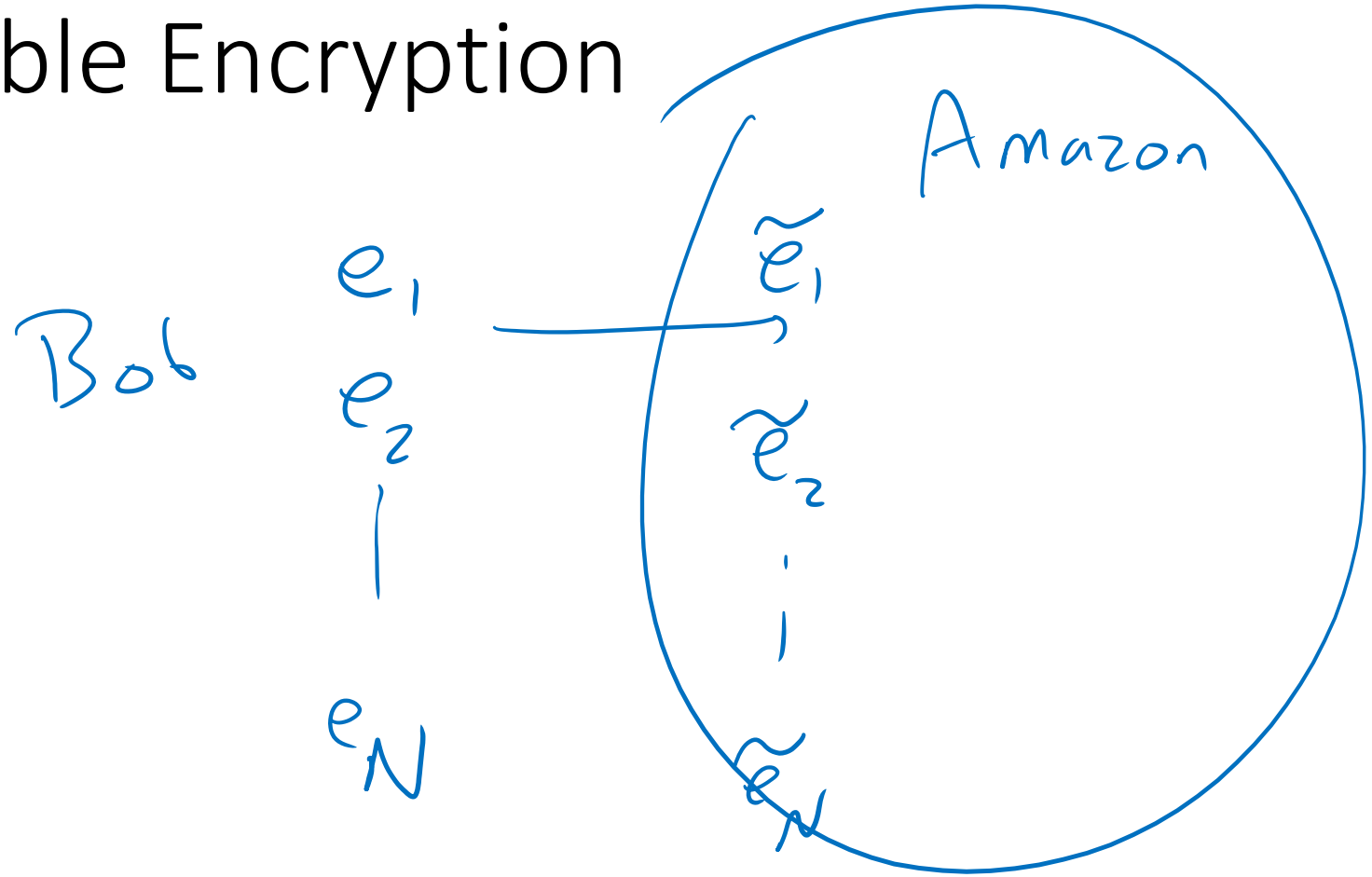
Amazon Cloud Service

Bob



es he wants $f(D)$.

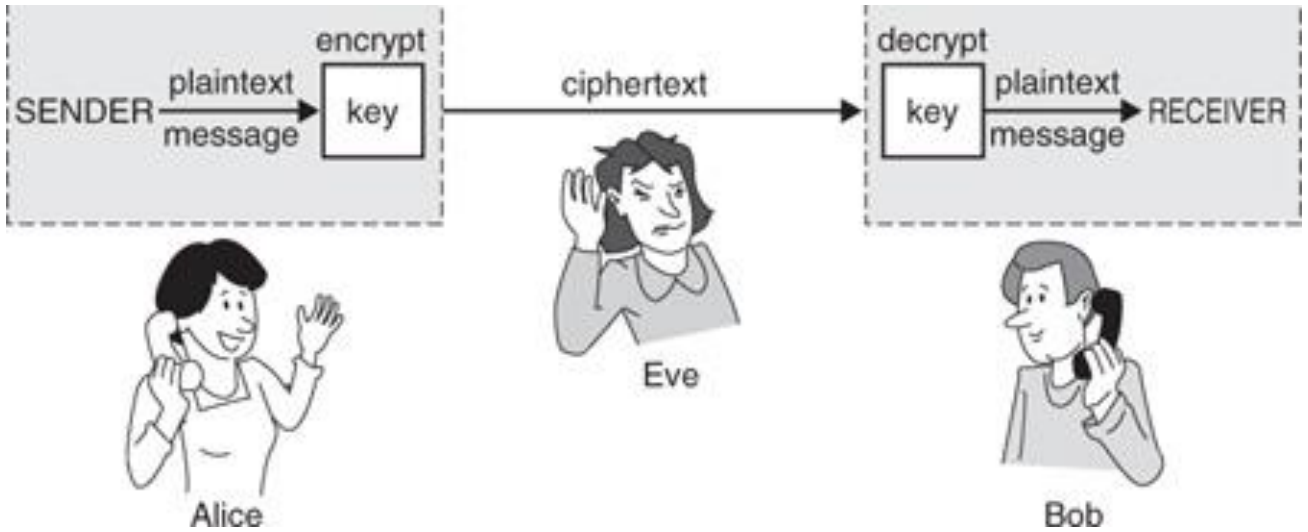
Searchable Encryption



And many more…

Encryption :
Perfect secrecy and its limitations

Privacy :


encrypt
SENDER
plaintext
message
key
ciphertext
decrypt
key
plaintext
message
RECEIVER
Alice
Eve
Bob

Chapters 1-2 of Katz-Lindell book

- Steganography and why it is not a good idea
- Defining Perfect Secrecy
- Problems with perfect secrecy

Setting for private-key encryption schemes

key. $k \in K$

$m \in M$

message

$c \in C$

ciphertext

- Alice and Bob share some "secret information" in advance

key: k

- They want to communicate a new message secretly.

- The communication happens in public.

Steganography

- Art of concealing the message in “innocent-looking” messages.

By **AMANDA SCHUPAK** / **CBS NEWS** / *January 27, 2015, 1:29 PM*

Use cat pictures to hide encrypted Facebook posts

Comment / Share / Tweet / Stumble / Email

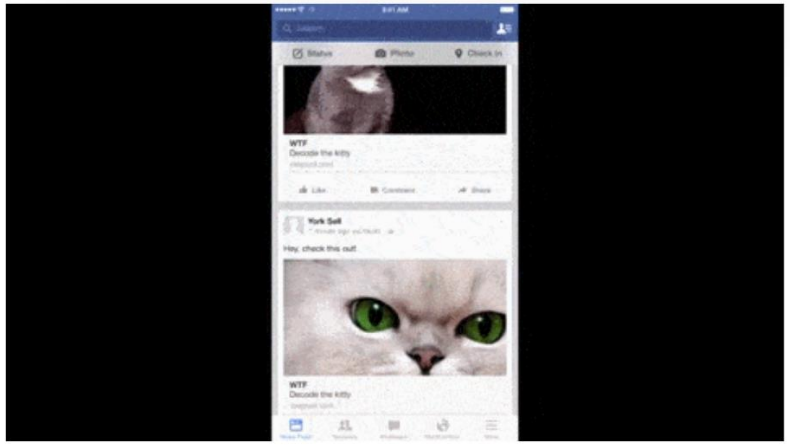


Image of a tree with a steganographically hidden image. The hidden image is revealed by removing all but the two least significant bits of each color component and a subsequent normalization. The hidden image is shown below.

Image of a cat extracted from the tree image above.

Steganography

- **Even the algorithm** used by Alice and Bob is hidden…

- When is it useful? ✓ When we want to hide the communication itself.

- What is wrong with it? As soon as algorithm leaks we need a new one!

Kerckhoffs's principle

The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.

Caesar cipher (weak variant)

- the i th letter is substituted with $(i + k)$ th letter.

$$c_i = E(p_i) = p_i + 3 \quad \text{mod } 26$$

A full translation chart of the Caesar cipher is shown here.

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Using this encryption, the message

TREATY IMPOSSIBLE

would be encoded as

T	R	E	A	T	Y		I	M	P	O	S	S	I	B	L	E
w	u	h	d	w	b		l	p	s	r	v	v	l	e	o	h

- Is it secure?

key length:
5 bits

Caesar Cipher (strong variant)

- Secret key: a random permutation over all letters.
- Key size: $\log(26!) > 88$ bits
- Is it now secure?