CS/ECE 578 CRYPTOGRAPHY AND DATA SECURITY

Köksal Muş

August 25,2021

WPI

OUTLINE

- **Administrative Details**
- Overview of Cryptography

ADMINISTRATIVE DETAILS

- Instructor: Koksal Mus, kmus@wpi.edu
  - Office hours: by appointment
- TA: Zane Weissman, zweissman@wpi.edu
  - Office hours: Thursdays 2-3 pm on Zoom
- Web Page : WPI Canvas
- Syllabus and textbook

ADMINISTRATIVE DETAILS

- **Grading**

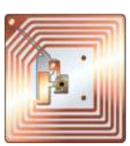
Exam(s):	%40
Assignments (5-6):	%40
Presentation(s):	%20

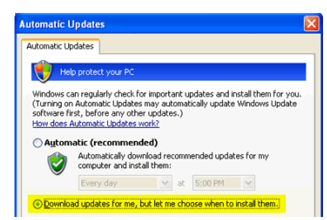
OUTLINE OF THE COURSE

- Symmetric Cryptography
  - Encryption
  - Authentication

- Asymmetric Cryptography
  - Key Exchange
  - Encryption
  - Digital signatures

- Applications of Cryptography





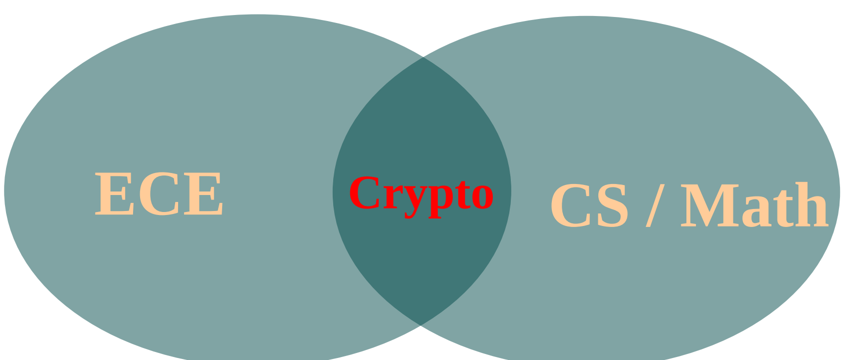
WHAT IS CRYPTOGRAPHY?

kryptos (Greek): "hidden, secret“

gráphein (Greek): "writing"

Cryptography:

- Science of *secure* data handling (transmission, storage, etc.)
- Achieves *confidentiality*, *authenticity* and *integrity* of data by applying mathematical algorithms
- Backbone of IT infrastructure and e-commerce



WHAT IS CRYPTANALYSIS?

kryptos (Greek): "hidden, secret“

analýein (Greek): "to loosen"

Cryptanalysis:

- To reach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown
  - Kerckhoffs’ principle
  - Shannon’s Assumption

Kerckhoffs' Principle

The security of the encryption scheme must depend only on the secrecy of the key k, and not on the secrecy of the algorithm

(1883 Auguste Kerckhoffs, one of six rules!)

Or by Claude Shannon:

"The enemy knows the system."

by Murphy:

"If there's more than one way to do a job and one of those ways will end in disaster, then somebody will do it that way."

SHANNON CIPHER AND PERFECT SECURITY

- A **Shannon cipher** is a pair $\mathcal{E} = (E, D)$ of functions.
- The function E (the **encryption function**) takes as input a **key** k and a **message** m (also called a **plaintext**), and produces as output a **ciphertext** c. That is, $c = E(k, m)$ and we say that c is the encryption of m under k.
- The function D (the **decryption function**) takes as input a key k and a ciphertext c, and produces a message m. That is, $m = D(k, c)$, and we say that m is the **decryption of** c **under** k.
- We require that decryption "undoes" encryption; that is, the cipher must satisfy the following **correctness property**: for all keys k and all messages m, we have $D(k, c) = D(k, E(k, m)) = m$.
- More Formally:

$$E = \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$$
$$D = \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$$

$\mathcal{E}$ is defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$

WHAT IS A "SECURE" CIPHER?

- A secure cipher is one for which an encrypted message remains "well hidden," even after seeing its encryption. Which means that it is hard to completely determine m from c, without knowledge of k.
- We assume that the adversary does know the encryption algorithm and the distribution of k

PERFECT SECURITY

- Let $\mathcal{E} = (E, D)$ be a Shannon cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. Consider a probabilistic experiment in which the random variable k is uniformly distributed over $\mathcal{K}$.

If for all $m_0, m_1 \in \mathcal{M}$, and all $c \in \mathcal{C}$, we have

$$\Pr[E(\boldsymbol{k}, m_0) = c] = \Pr[E(\boldsymbol{k}, m_1) = c],$$

then we say that $\mathcal{E}$ is a perfectly secure Shannon cipher.

EX: *The one-time pad is a perfectly secure Shannon cipher.*

- $\mathcal{K} \coloneqq \mathcal{M} \coloneqq \mathcal{C} \coloneqq \{0,1\}^L$
- $c = k \oplus m$

EX: *Variable length one-time pad is not a perfectly secure Shannon cipher.*

- $\mathcal{K} := \mathcal{M} := \mathcal{C} := \{0,1\}^x$
- $c = k \oplus m$

$$m_1 = '11' \rightarrow E(11)$$
$$m_2 = '110' \rightarrow E(110)$$

SHANNON'S THEOREM

- *Let $\mathcal{E} = (E, D)$ be a Shannon cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. If $\mathcal{E}$ is perfectly secure, then $|\mathcal{K}| \geq |\mathcal{M}|$.*

- The only way to achieve perfect security is to have keys that are as long as messages

COMPUTATIONAL CIPHER AND SEMANTIC SECURITY

- $|\Pr[\phi(E(k,m_0))] - \Pr[\phi(E(k,m_1))]| \leq \varepsilon$ for some very small or negligible value of ε

- New definition of security should be flexible enough to allow ciphers with variable length message spaces to be considered secure so long as they do not leak any useful information about an encrypted message to an adversary *other than the length of message*.

ATTACKS BY SCENARIOS

- **Ciphertext only attack:** Eve only knows ciphertexts.
- **Known plaintext attack:** Eve knows (parts of) plaintext in addition to full cipher-text (e.g. encoding/beginning of email).
- **Chosen plaintext attack:** Eve has access to an encryption "device" (oracle) that can encrypt arbitrary messages.
- **Chosen ciphertext attack:** Eve has access to decryption oracle, i.e. can decrypt arbitrary messages.

HISTORY OF CRYPTOGRAPHY

- 50 B.C. Julius Caesar: Caesar-Cipher

- 1587 : Mary Stuart: Substitution Cipher

  → **Cryptanalysis** results in execution

	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
A	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
B	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	A
C	C	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
D	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

- 19^{th} century: Vigenère works on polyalphabetic ciphers

HISTORIC CIPHERS

- Caesar Cipher (Shift Cipher)
- Substitution Cipher
- Vigenère Cipher

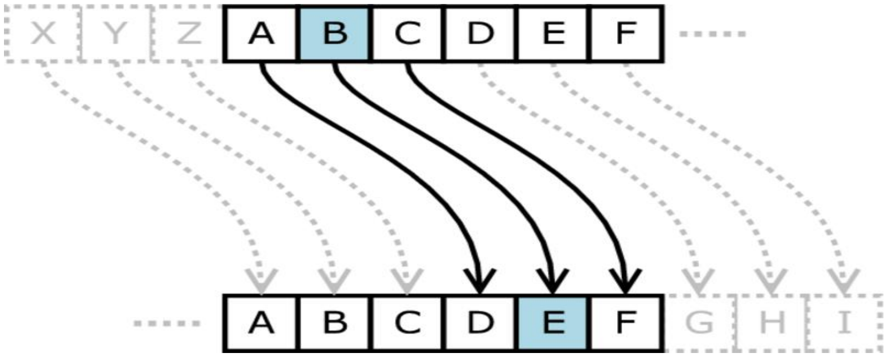
CAESAR'S CIPHER (SHIFT CIPHER)

Scheme: shift every letter in the alphabet (message space) by a fixed number of positions.

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

CAESAR CIPHER (SHIFT CIPHER)

Shifting each letter of the alphabet by a fixed offset: A→D, B→E …



E.g.: **CAR → FDU**

Problems:

- Security by obscurity
- Key space is too small (26 possible offsets)

CRPYTANALYSIS OF CAESAR'S CIPHER

Brute Force Attack (**exhaustive key search**):

Try all possible shifts (26 shifts, easily done).

- Given a (few) (m_i, c_i) such that $c_i = Enc_k(m_i)$.
- Check "all" $k \in K = \{k_1, k_2, \cdots, k_n\}$.
- If $c_i = Enc_{k^*}(m_i)$, then $k = k^*$ with high probability.
- Execution time: $O(|K|)$
- Key Space: In this case, the key space is too small ($|\mathrm{K}| = 26$).
- Any cryptosystem must have key space large enough to resist exhaustive key search, typical 128~256 bits.

SUBSTITUTION CIPHER

Replace each letter of the message according to a substitution table:

Plain: **abcdefghijklmnopqrstuvwxyz**
Cipher: **PASWORDBCEFGHIJKLMNQTUVXYZ**

E.g.: **car→ SPM**

Key Space: it is large enough. $|K| = 26! \sim 2^{88}$

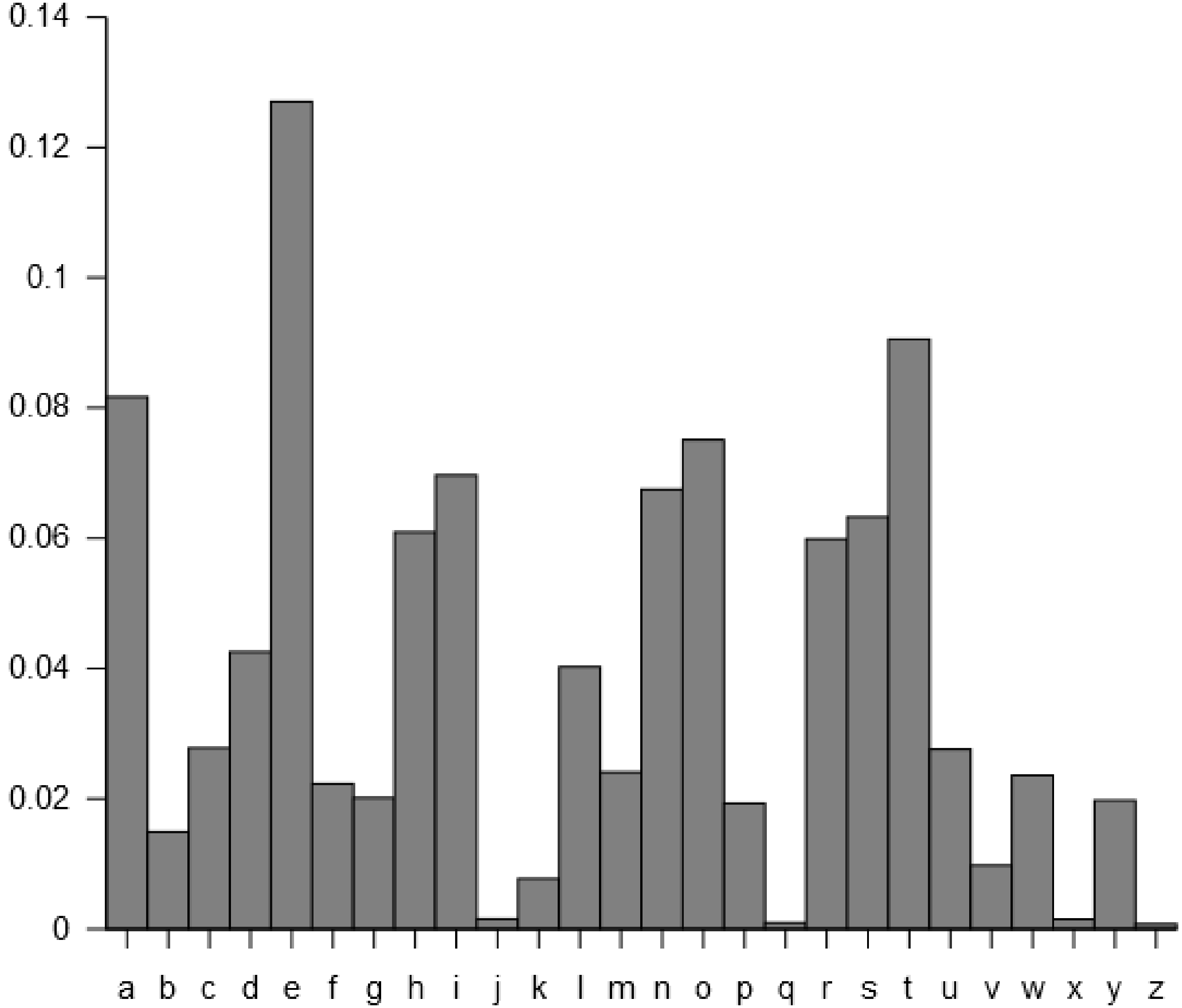
CRYPTANALYSIS OF SUBSTITUTION CIPHER

Key Space: it is large enough.
$|K| = 26! \sim 2^{88}$

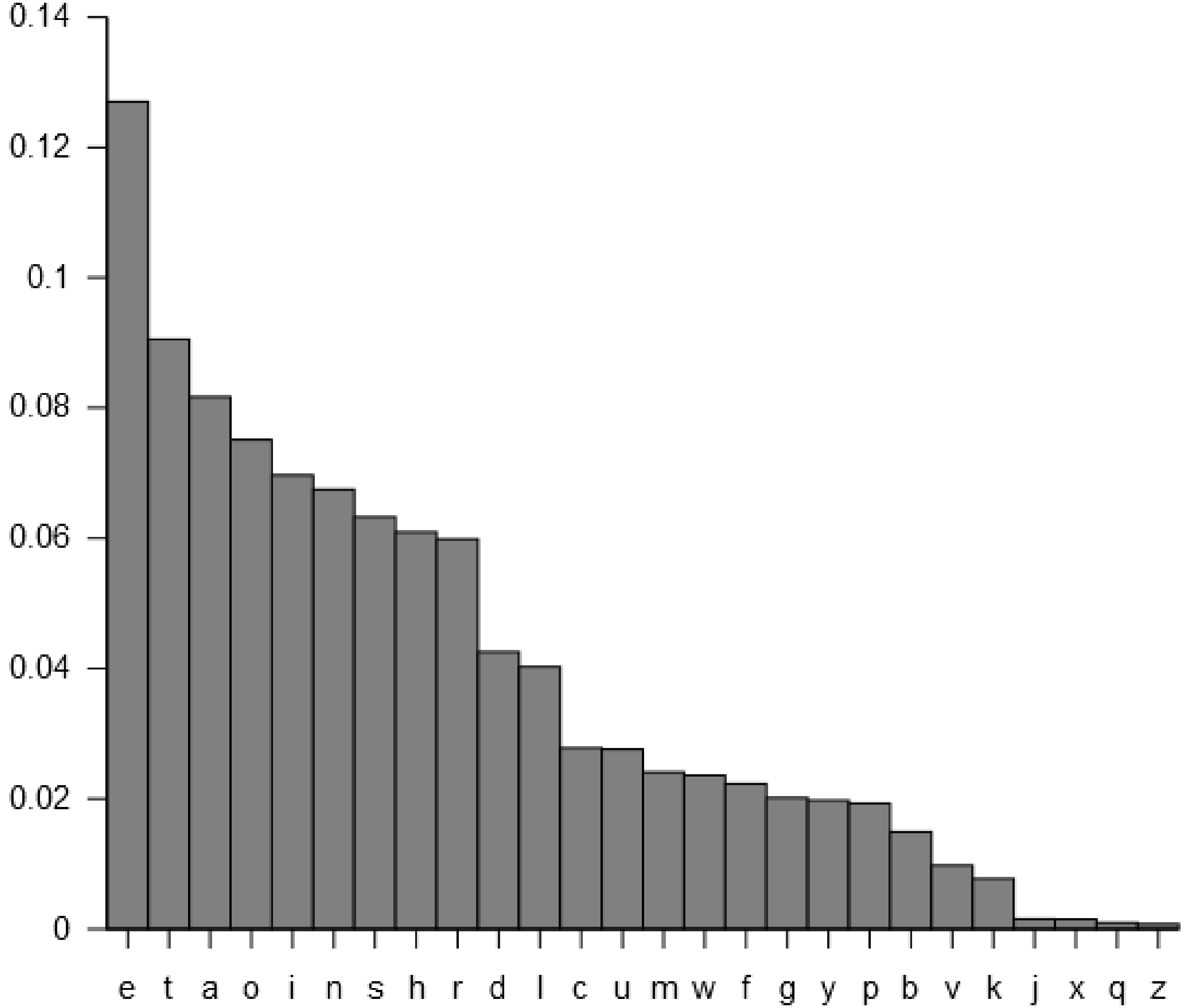
Is this secure?
No*! Mono-alphabetic cipher can be easily attacked with "Letter Frequency Analysis".

*Large key space is not enough to provide security.

LETTER FREQUENCIES



LETTER FREQUENCIES



VIGENÈRE CIPHER

- a.k.a. *the indecipherable cipher*
- Combines several Caesar ciphers:
  - Different shift for different letter positions

Plaintexts

Keys

	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
A	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
B	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	A
C	C	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
D	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

ity

key = ‘**car**’, message = ‘**hello**’:

H → J (key: a→c, shift by 2)

E → E (key: a→a, shift by 0)

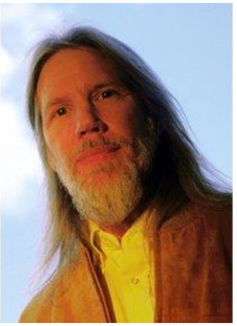
L → C (key: a→r, shift by 17)

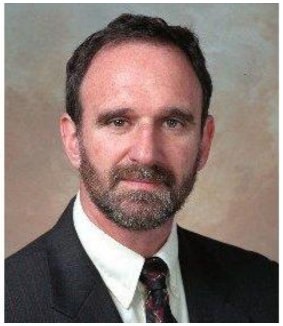
L → N (key: a→c, shift by 2)

O → O (key: a→a, shift by 0)

Why do we need Modern Cryptography ?

CRYPTOGRAPHY TODAY



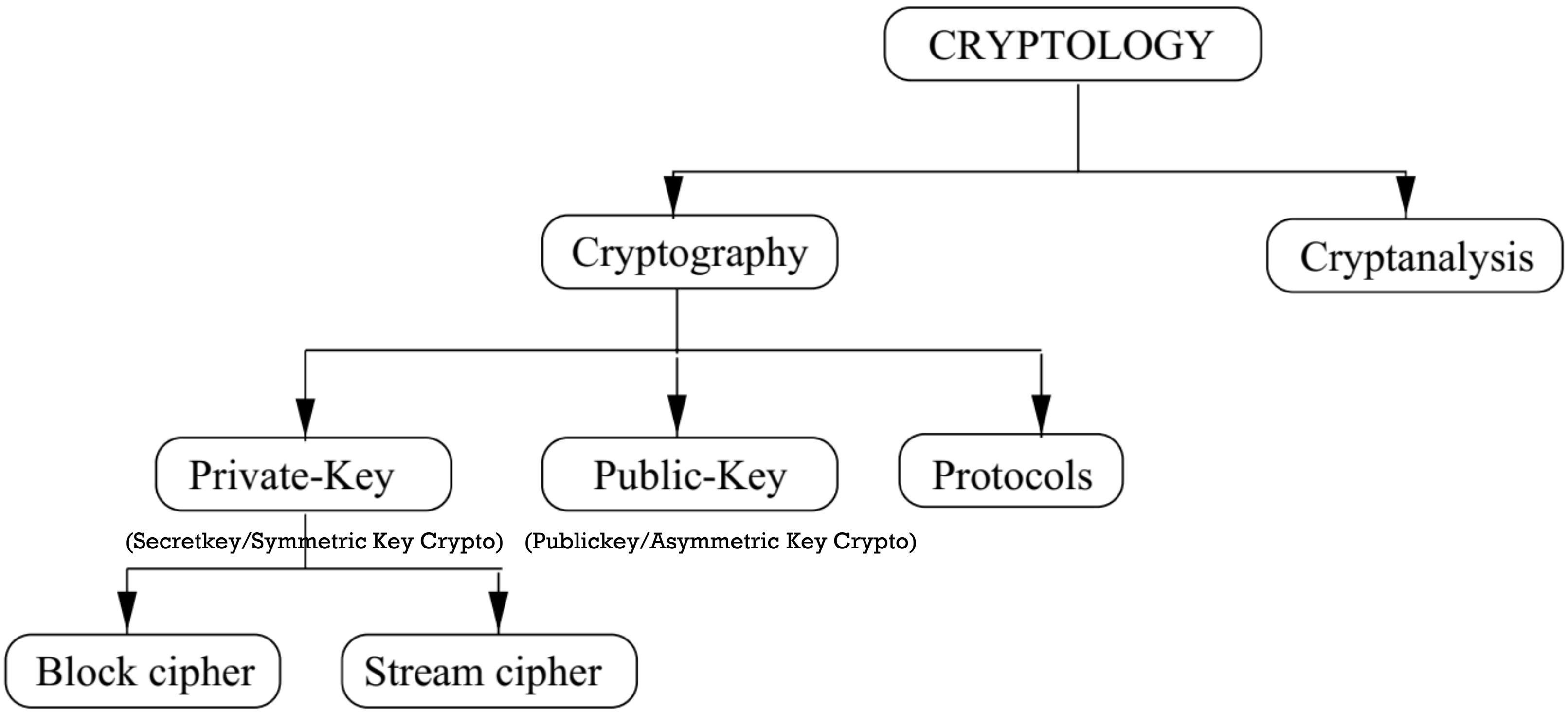


- Public Key Cryptography(mid 70s):
  - Achieves *confidentiality*, *authenticity* and *integrity* in open environments: **Internet**
  - Digital Signatures: **enables e-Commerce**

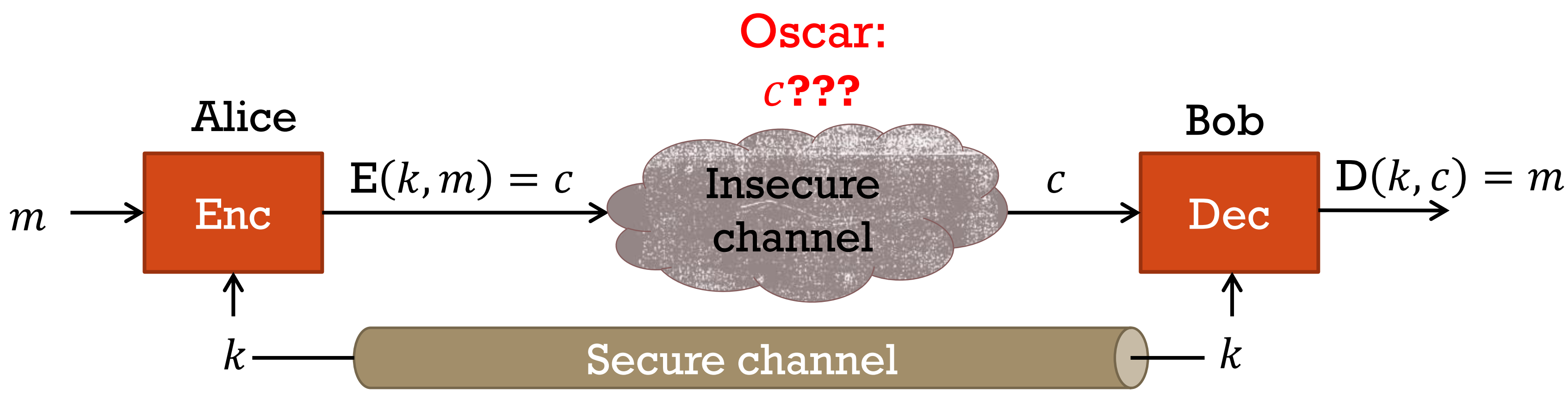
Digital revolution turns cryptography into a Science:

- Cryptography: Building secure ciphers based on mathematical principles
- Cryptanalysis (*"Code Breaking"*): Studying weaknesses of ciphers

OVERVIEW ON THE FIELD OF CRYPTOLOGY



SYMMETRIC ENCRYPTION



E, D: cipher k: secret key (shared secret, 128…256bit)

m: message (plaintext)

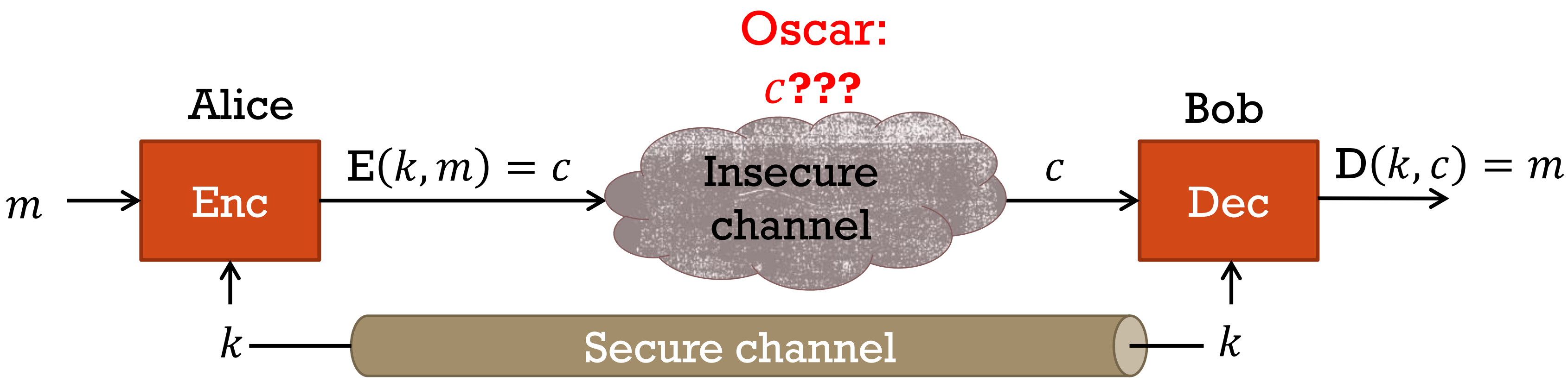
c: ciphertext: no info about m → c looks random

- Security Service: **Secrecy** (a.k.a. **Confidentiality**)

- Cipher is publicly known (Kerckhoffs' Principle)

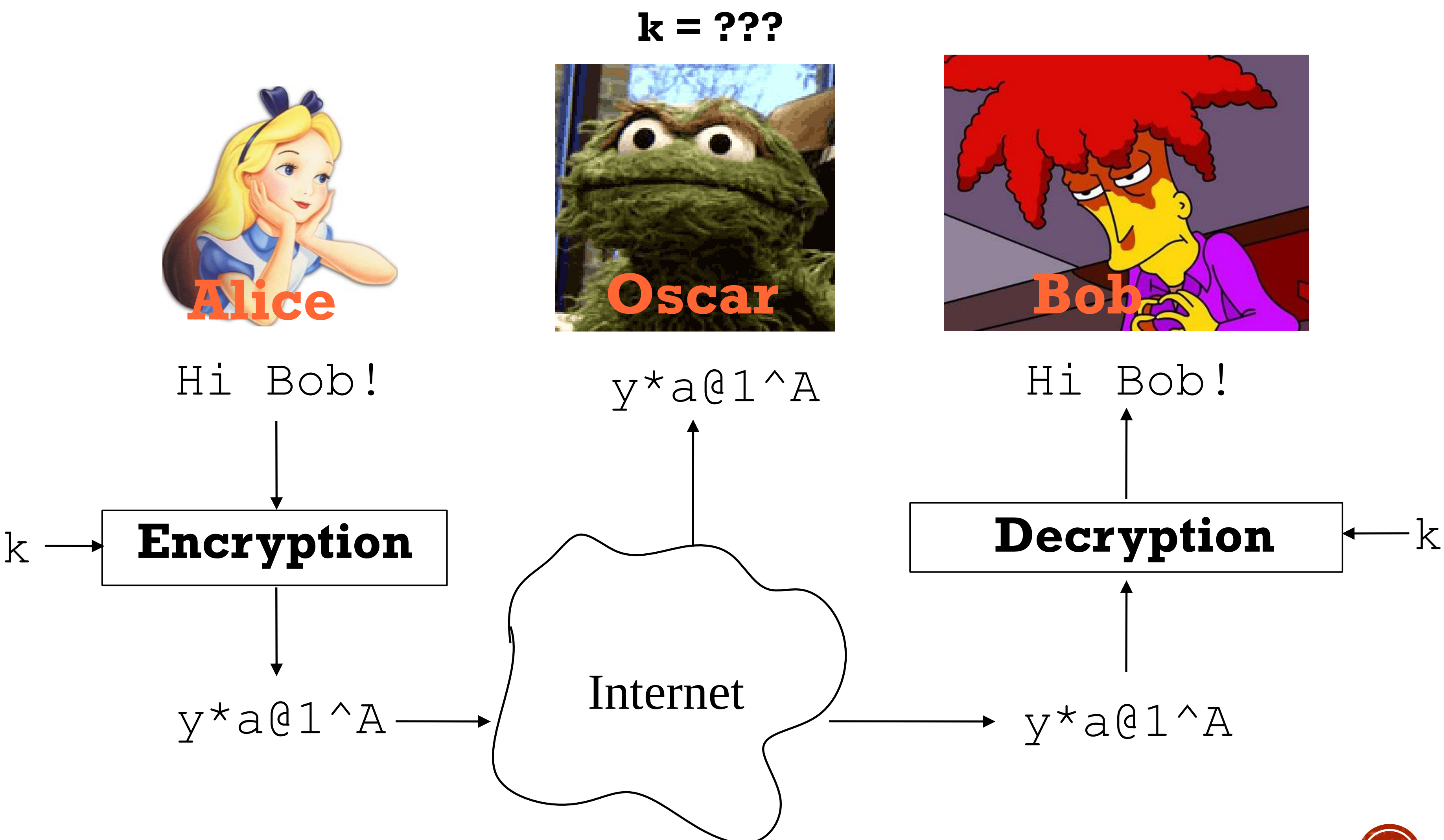
  → Security by Obscurity is setup for failure!

SYMMETRIC ENCRYPTION



Analogous to strongbox

ENCRYPTION AND DECRYPTION



STREAM CIPHERS

Enc: $c_i = m_i \oplus s_i$

Dec: $m_i = c_i \oplus s_i$

Gen: $k \leftarrow \{0,1\}^n$

k: secret key (shared secret, 128…256bit)

s_i: key stream

- Uses key stream generator to turn short key k into long (pseudo) random sequence s_i
- \+ Low latency for encryption/decryption Encryption
- \+ Enc = Dec → simple
- \- **Malleable:** Adversary can flip bits to change message (doesn't break secrecy)
- **How to build a key stream generator?**

WHY DO WE NEED ASYMMETRIC KEY CRYPTOGRAPHY?

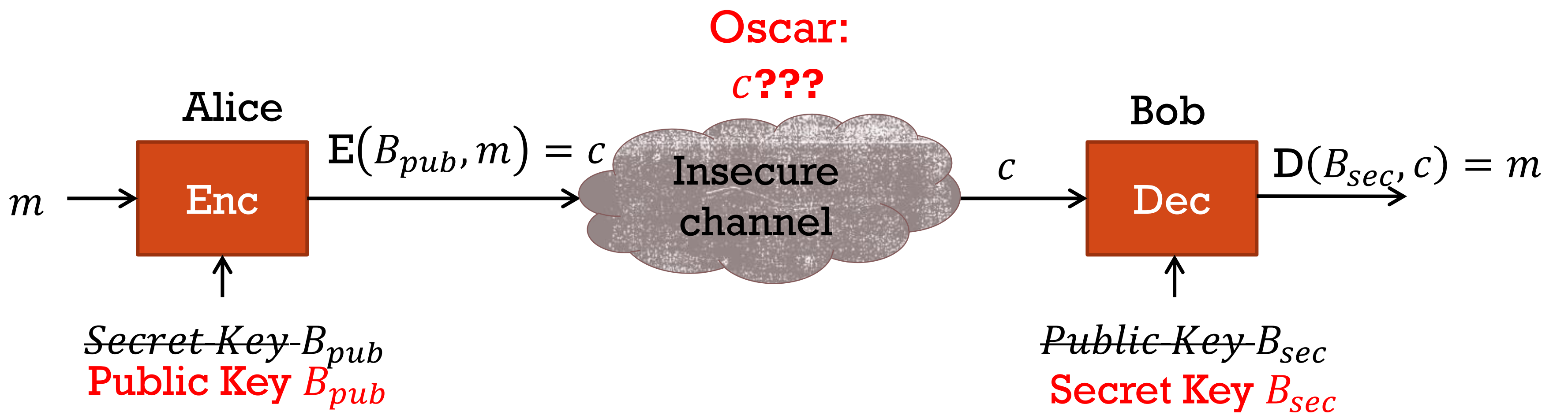
Asymmetric Encryption

	Public Key	Secret Key
Alice	A_{pub}	A_{sec}
Bob	B_{pub}	B_{sec}

ASYMMETRIC ENCRYPTION

Analogous to

ASYMMETRIC ENCRYPTION

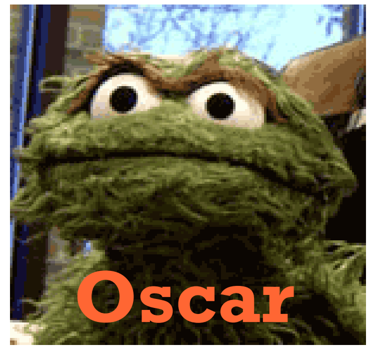


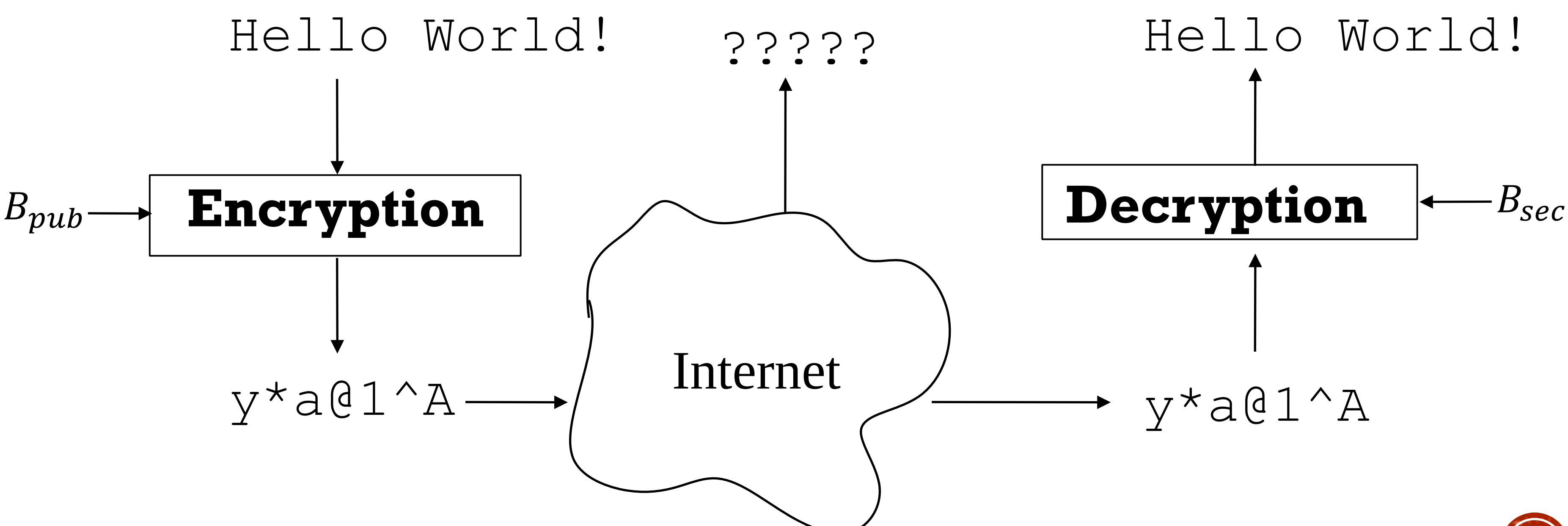
	Public Key	Secret Key
Alice	A_{pub}	A_{sec}
Bob	B_{pub}	B_{sec}

ASYMMETRIC KEY ENCRYPTION AND DECRYPTION

	Public Key	Secret Key
Alice	A_{pub}	A_{sec}
Bob	B_{pub}	B_{sec}

k = ???

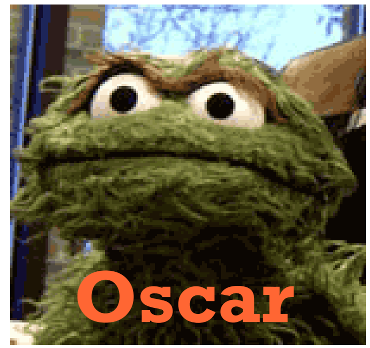


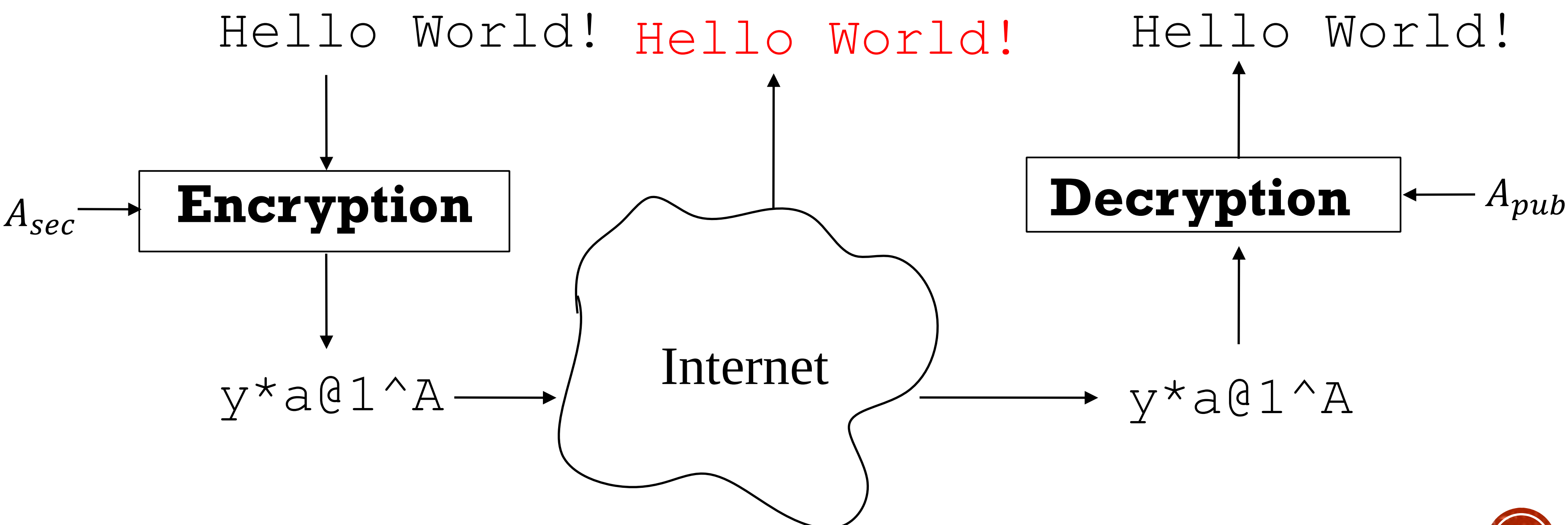


ASYMMETRIC KEY ENCRYPTION AND DECRYPTION

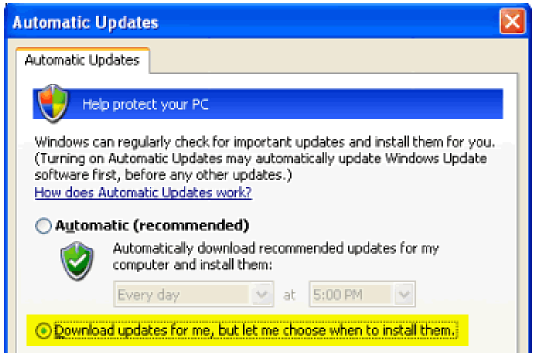
	Public Key	Secret Key
Alice	A_{pub}	A_{sec}
Bob	B_{pub}	B_{sec}

$k = A_{pub}$

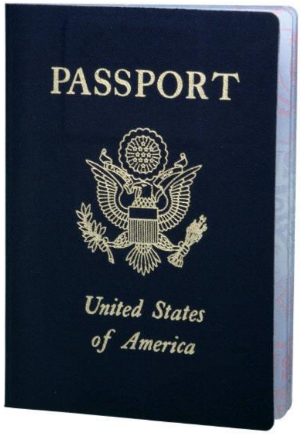


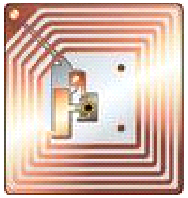


APPLICATIONS OF CRYPTOGRAPHY



Wi Fi™
ZONE





THANK YOU FOR YOUR ATTENTION!

Dr. Köksal
Muş

kmus@wpi.edu