CSC429 – Computer Security

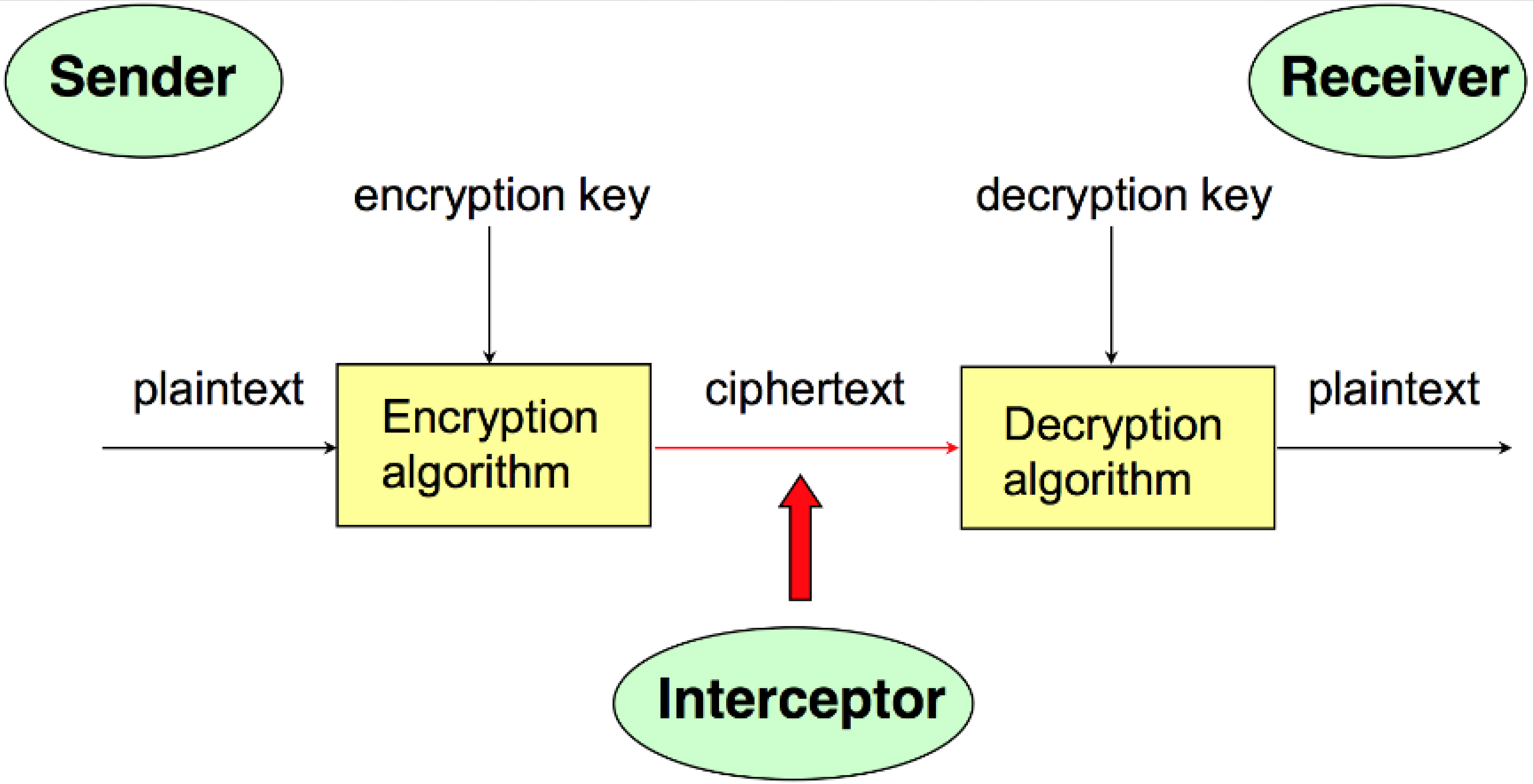
LECTURE 2
INTRODUCTION TO CRYPTOGRAPHY

Mohammed H. Almeshekah, PhD
meshekah@ksu.edu.sa

Notes

- Make sure you have access to Piazza.

A Cryptosystem



Three Important Questions

- Can cryptography prevent a communication from being intercepted?

- Which of the following must be kept secret?
  1. Encryption algorithm
  2. Decryption algorithm
  3. Encryption key
  4. Decryption key

- Does using a good encryption algorithm guarantee the confidentiality of a message?

Models for Evaluating Security

- Unconditional (information-theoretic) security:
  - Adversary has unlimited resources.
  - Scheme that achieve such level is **perfectly secret**.
  - Analysis is done using probability theory.

- Computational Security:
  - Measures the amount of computational effort to defeat the system.
  - Usually based on difficult mathematical problems (e.g. discrete logarithm, factoring, etc).

Classical Ciphers

Shift Cipher

- Each letter is shifted by **K** positions.
  - Can be modeled as a addition modulo 26.

- Encryption:
  - Shift to the right by K.
- Decryption:
  - Shift to the left by K.

- History:
  - Caesar cipher – [K = 3].

Shift Cipher - 2

- 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
- 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- Example:
  - P = CRYPTOGRAPHYISFUN
  - K = 11
  - C = NCJAVZRCLASJTDQFY

- What is the key space?

- How can you brake it?

Mono-alphabetical Substitution Cipher

- The key space: all permutations of $\Sigma = \{A, B, C, \ldots, Z\}$
- Encryption given a key π:
  - each letter X in the plaintext P is replaced with $\pi(X)$
- Decryption given a key π:
  - each letter Y in the ciphertext P is replaced with $\pi^{-1}(Y)$

Substitution Cipher - 2

- Example:

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

- BECAUSE → AZDBJSZ
- What is the key space?
- Can it be broken?

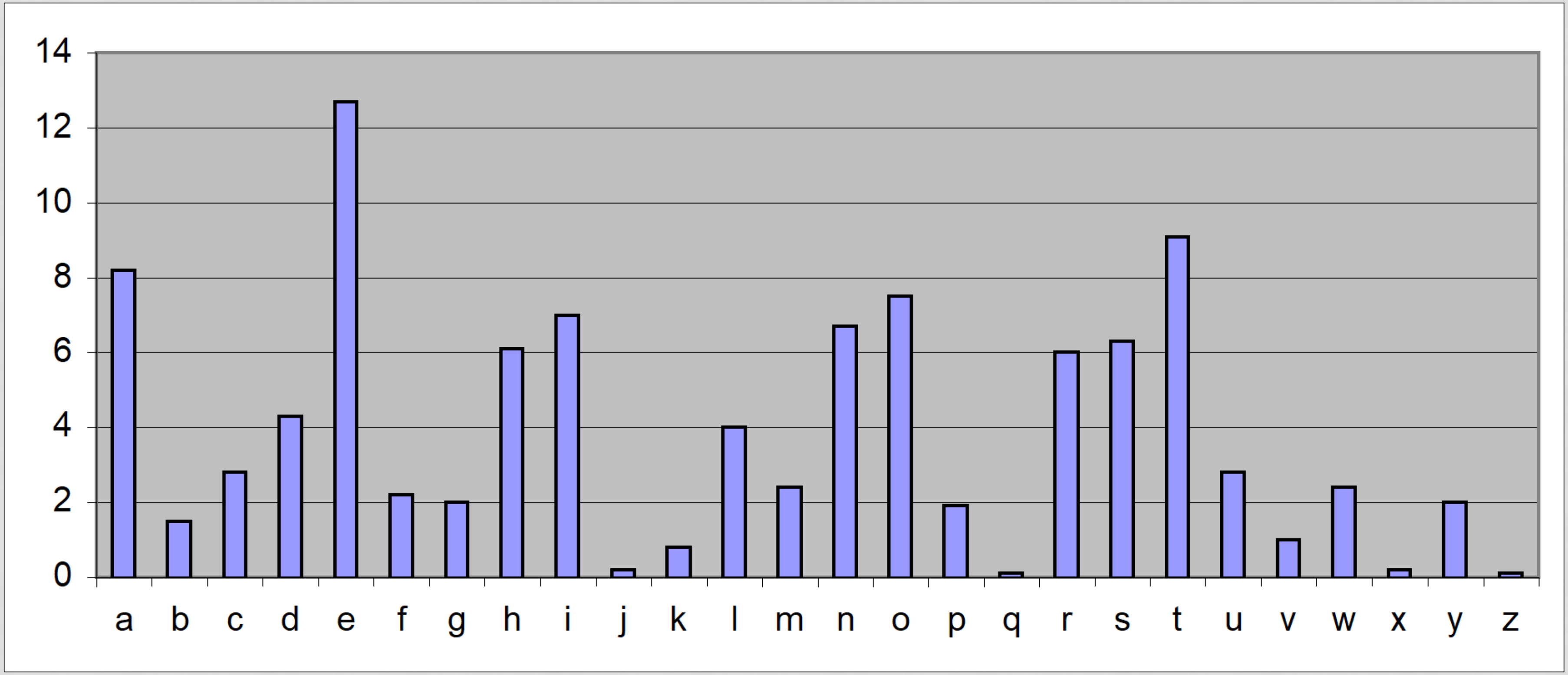
Breaking Substitution Cipher

- Each language has certain features - frequency of letters.

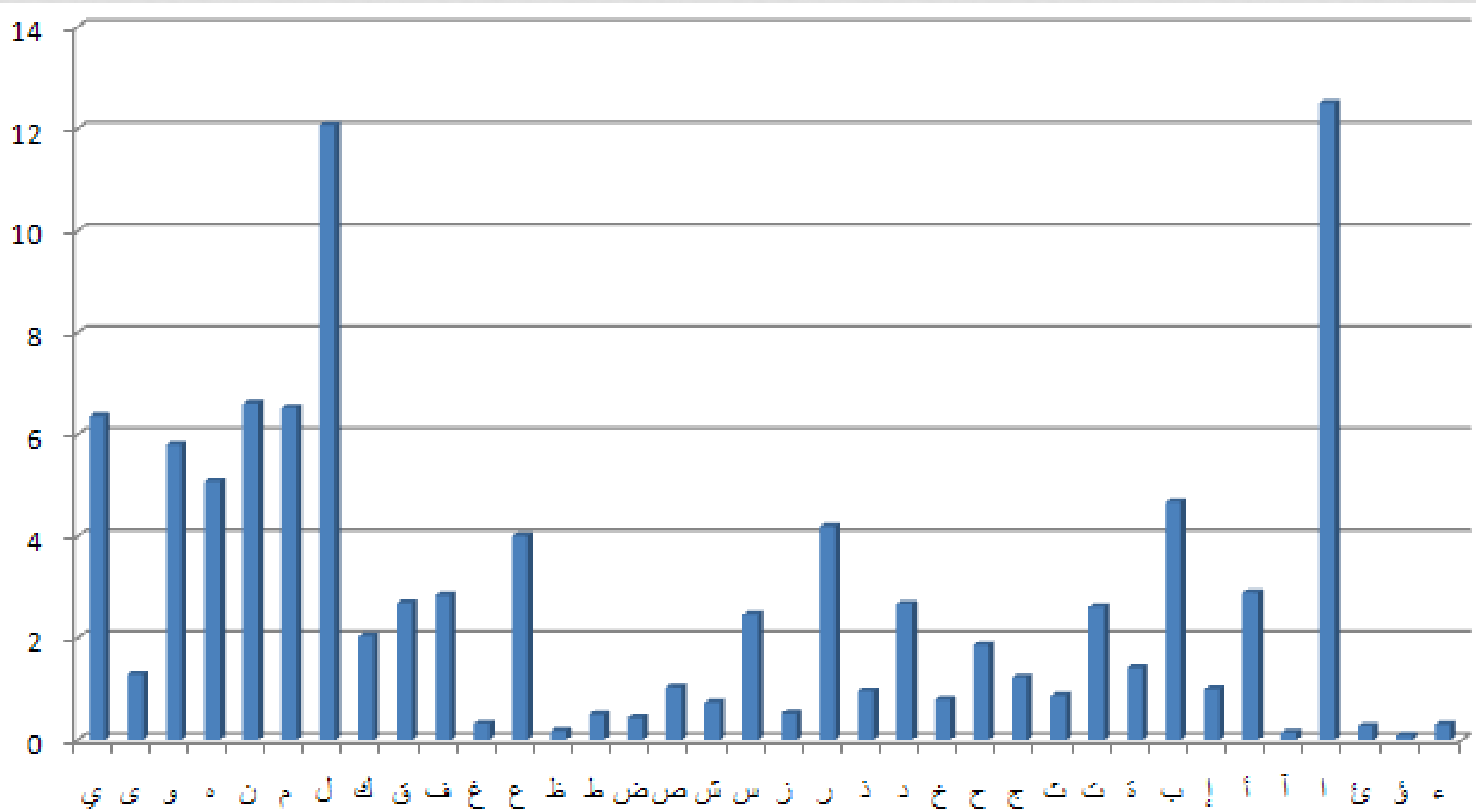
- Substitution ciphers preserve the language features.

- Substitution ciphers are vulnerable to frequency analysis attacks.

Frequency of Letters in English



Frequency of Letters in Arabic



Polyalphabetic Substitution Ciphers

- Main weaknesses of mono-alphabetic substitution ciphers:
  - Each letter in the ciphertext corresponds to only one letter in the plaintext letter

- Lesson:
  - A large key space alone doesn't guarantee security.

- Lead to the development Vigenère cipher.

The Vigenère Cipher

- Given m, a positive integer, $P = C = (Z_{26})^n$, and $K = (k_1, k_2, \ldots, k_m)$ a key, we define:
  - Encryption:
    - $E_k(p_1, p_2 \ldots p_m) = (p_1+k_1, p_2+k_2 \ldots p_m+k_m) \pmod{26}$
  - Decryption:
    - $D_k(c_1, c_2 \ldots c_m) = (c_1-k_1, c_2-k_2 \ldots c_m-k_m) \pmod{26}$

- Example:
  - Plaintext: C R Y P T O G R A P H Y
  - Key: L U C K L U C K L U C K
  - Ciphertext: N L A Z E I I B L J J I

Security of Vigenère Cipher

- Vigenère masks the frequency with which a character appears in a language: one letter in the ciphertext corresponds to multiple letters in the plaintext. Makes the direct use of frequency analysis more difficult.

- Is it secure?

Cryptanalysis of Vigenère Cipher

- Find the length of the key: (e.g. using Kasisky test).
- Divide the message into that many shift cipher encryptions.
- Use frequency analysis to solve the resulting shift ciphers.

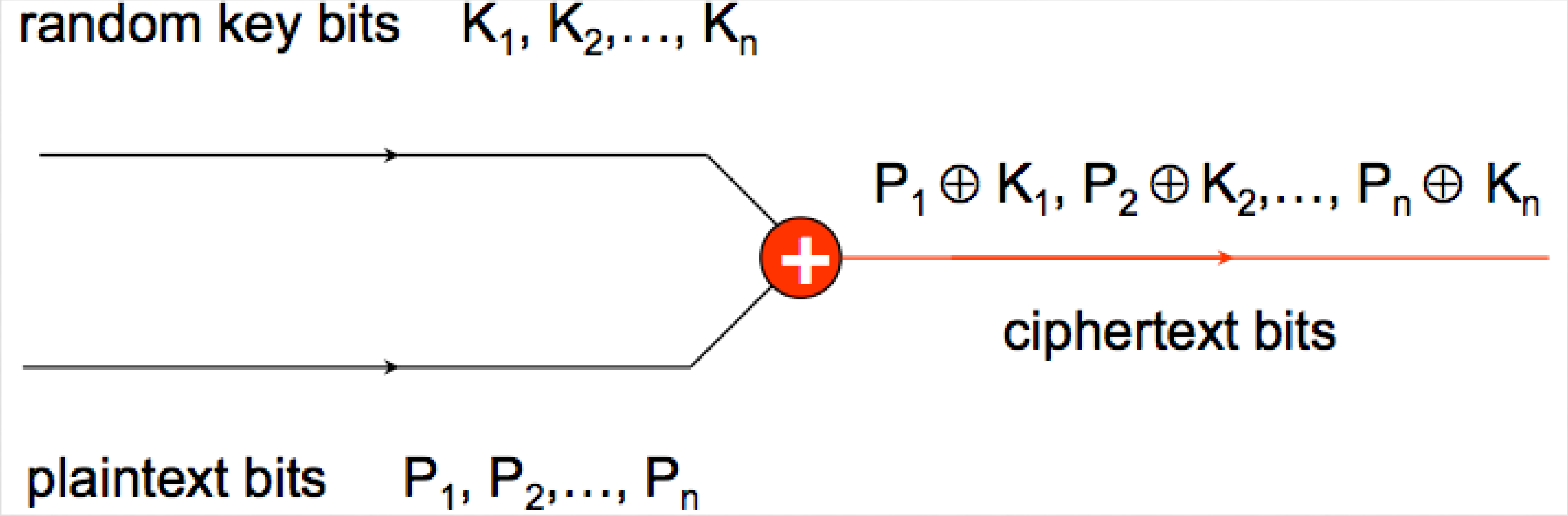
One-Time Pad (OTP)

- Key is a random string that is at least as long as the plaintext.
- Encryption is similar to shift cipher.
- Let Z_m ={0,1,…,m-1} be the alphabet.
  - Plaintext space = Ciphtertext space = Key space = $(Z_m)^n$
  - The key is chosen uniformly randomly
  - Plaintext $X = (x_1\ x_2\ \ldots\ x_n)$
  - Key $K = (k_1\ k_2\ \ldots\ k_n)$
  - Ciphertext $Y = (y_1\ y_2\ \ldots\ y_n)$
  - $E_k(X) = (x_1+k_1\ \ x_2+k_2\ \ldots\ x_n+k_n) \bmod m$
  - $D_k(Y) = (y_1-k_1\ \ y_2-k_2\ \ldots\ y_n-k_n) \bmod m$

One-Time Pad (OTP) - 2

- Key must be:
  - As long as the plaintext.
  - Random.
  - Not be re-used.

- Binary Version:



Next Lecture

- We will start discussing modern cryptography.
- Readings for next lecture:
  - Anderson's book – (5.3.2) and (5.3.3).