CSC 519 Information Security

LECTURE 2: Cryptography

Dr. Esam A. Alwagait
alwagait@ksu.edu.sa

Module 2: Elementary Cryptography

- Concepts of Encryption
- Cryptanalysis: how encryption systems are broken
- Symmetric (secret key) encryption and the DES and AES algorithms
- Asymmetric (public key) encryption and the RSA algorithm
- Key exchange protocols and certificates
- Digital signatures
- Cryptographic hash functions

Concepts of Encryption

- Cryptography is rooted in higher mathematics:
  - group and field theory
  - computational complexity
    - E.g. the question of the extent to which a problem is solvable on a computer
  - real analysis
    - the theory of functions of a real variable
- In addition to probability and statistics

Concepts of Encryption

- Consider the steps involved in sending messages from a sender, S, to a recipient, R
- If **S** entrusts the message to T, who then delivers it to **R**, **T** then becomes the transmission medium.
- If an outsider, O, wants to access the message (to read, change, or even destroy it), we call **O** an interceptor or intruder

Concepts of Encryption

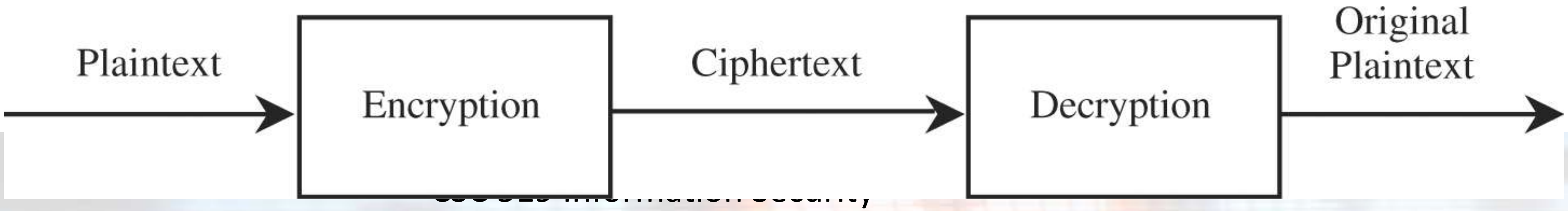
- **O** might try to access the message in any of the following ways:
- Block it, by preventing its reaching **R**, thereby affecting the availability of the message.
- Intercept it, by reading or listening to the message, thereby affecting the confidentiality of the message.
- Modify it, by seizing the message and changing it in some way, affecting the message's integrity.
- Fabricate an authentic-looking message, arranging for it to be delivered as if it came from **S**, thereby also affecting the integrity of the message
- A message's vulnerabilities reflect the four possible security failures we identified earlier.

Terminology

- **Encryption** is the process of encoding a message so that its meaning is not obvious
- **Decryption** is the reverse process, transforming an encrypted message back into its normal, original form
- Alternatively, the terms **encode** and **decode** or **encipher** and **decipher** are used instead of encrypt and decrypt
- We say that we encode, encrypt, or encipher the original message to hide its meaning
- We decode, decrypt, or decipher it to reveal the original message
- A system for encryption and decryption is called a **cryptosystem**

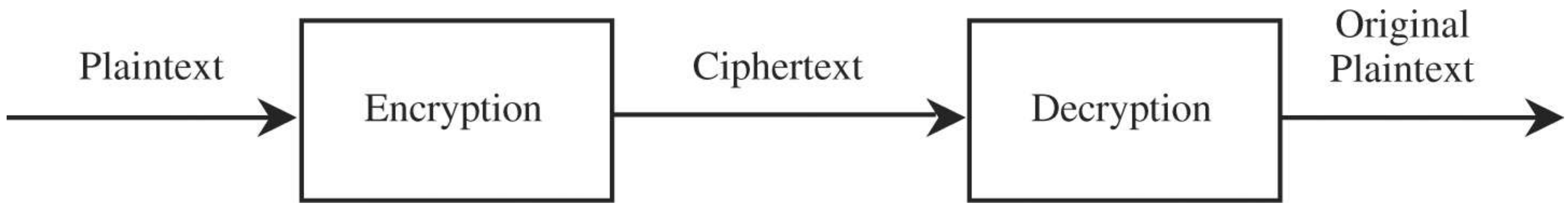
Terminology

- Slight difference (not significant in this course):
- **encoding** is the process of translating entire words or phrases to other words or phrases
- **enciphering** is translating letters or symbols individually
- **encryption** is the group term that covers both encoding and enciphering



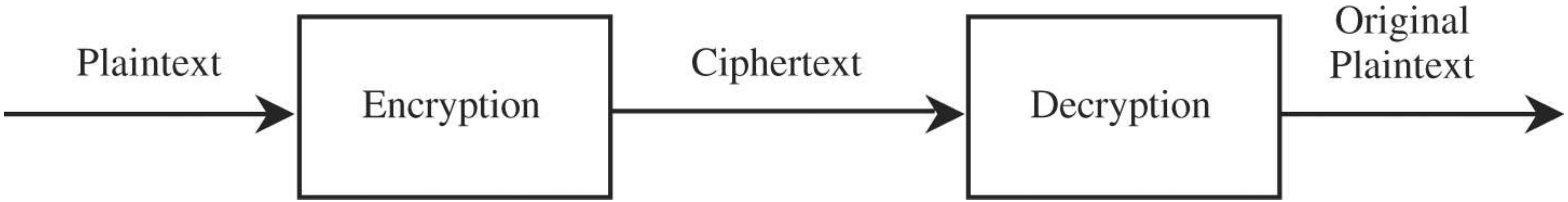
Terminology

- The original form of a message is known as **plaintext**
- The encrypted form is called **ciphertext**
- We denote a plaintext message **P** as a sequence of individual characters $\mathbf{P} = \langle p_1, p_2, \ldots, p_n \rangle$
- Similarly, ciphertext is written as $\mathbf{C} = \langle c_1, c_2, \ldots, c_m \rangle$



Terminology

- Example:
  - The plaintext message "I want cookies" can be denoted as the message string <I, ,w,a,n,t, , c,o,o,k,i,e,s>
  - It can be transformed into ciphertext <c_1, c_2, …, c_{14}>, and the encryption algorithm tells us how the transformation is done



Terminology

- We use this formal notation to describe the transformations between plaintext and ciphertext
- We write $C = E(P)$ and $P = D(C)$, where
  - C represents the ciphertext
  - E is the encryption rule
  - P is the plaintext, and D is the decryption rule
- What we seek is a cryptosystem for which $P = D(E(P))$
- In other words, we want to be able to convert the message to protect it from an intruder, but we also want to be able to get the original message back so that the receiver can read it properly

Terminology

- The cryptosystem involves a set of rules for how to encrypt the plaintext and how to decrypt the ciphertext
- The encryption and decryption rules, called **algorithms**, often use a device called a **key**, denoted by **K**, so that the resulting ciphertext depends on the original plaintext message, the algorithm, and the key value
- We write this dependence as $C = E(K, P)$
- This process is similar to using mass-produced locks in houses!
  - Expensive if every lock is designed separately
  - Few well-known companies produce standard locks that differ according to the key!

Terminology

- **Cryptography** means hidden writing using encryption to conceal text
- A **cryptanalysis** is studying encryption and encrypted messages, hoping to find the hidden meanings
- Both a **cryptographer** and a **cryptanalyst** attempt to translate coded material back to its original form
- But, a cryptographer normally works on behalf of a legitimate sender or receiver,
- whereas a cryptanalyst works on behalf of an unauthorized interceptor
- **Cryptology** is the research into and study of encryption and decryption
  - it includes both cryptography and cryptanalysis

Concepts

- Cryptography – hidden writing

- Encryption – encode or encipher
- Decryption – decode or decipher

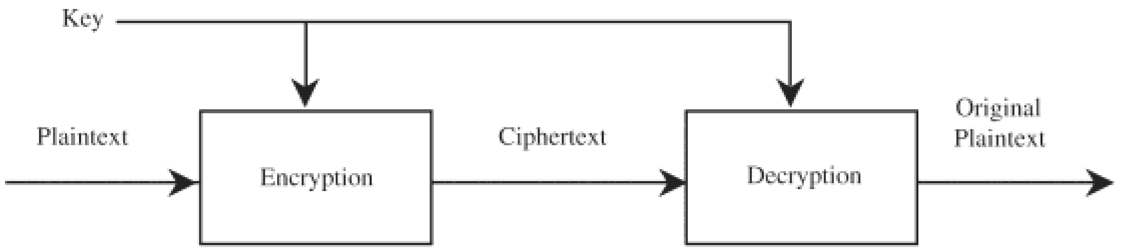
- Cryptosystem – a system for encryption and decryption

- Cryptographer – anyone who invents encryption algorithms
- Cryptanalyst – anyone who attempts to break encryption algorithms

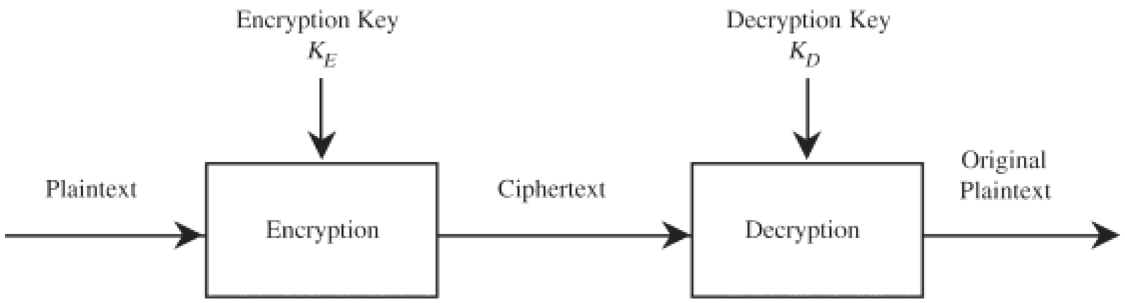
- Cryptology – research of encryption and decryption, including both cryptography and cryptanalysis

Concepts of symmetric and asymmetric encryption

- **Symmetric** : the encryption and decryption keys are the same, so
  - P = D(K, E(K,P)).
  - D and E are mirror-image processes
- **Asymmetric**: encryption and decryption keys come in pairs. Then, a decryption key, K_D, inverts the encryption of key K_E so that
  - $P = D(K_D, E(K_E,P))$
  - converting C back to P involves a series of steps and a key that are different from the steps and key of E



(a) Symmetric Cryptosystem



(b) Asymmetric Cryptosystem

Why using a key?

- We can create different encryptions of one plaintext message just by changing the key
- Using a key provides additional security
  - If the encryption algorithm should fall into the interceptor's hands, future messages can still be kept secret because the interceptor will not know the key value

What can a cryptanalyst attempt to do?

- Break a single message
- Recognize patterns in encrypted messages
  - to be able to break subsequent ones by applying a straightforward decryption algorithm
- Infer some meaning without even breaking the encryption
  - such as noticing an unusual frequency of communication or determining something by whether the communication was short or long
- Deduce the key
  - to break subsequent messages easily
- Find weaknesses in the implementation or environment of use of encryption
- Find general weaknesses in an encryption algorithm, without necessarily having intercepted any messages

What can a cryptanalyst attempt to do?

- Cryptanalyst cannot be expected to try only the hard, long way!
  - analyst can use educated guesses combined with careful analysis to generate all or most of an important message
  - Example: WWII 1942 (AF for Midway island between US and Japanese)
- Estimates of breakability are based on current technology, not future!
- Things that were infeasible in 1940 became possible by the 1950s
- Remember "Moore's Law"
  - the speed of processors doubles every 1.5 years, and this conjecture has been true for over two decades

Representing Characters

- Use the mathematical form below
- The letter A is represented by a zero, B by a one, and so on
- We can perform simple modular arithmetic on letters using the corresponding code numbers
- A + 4 = E,   K - 2 = I,   Y + 3 = B

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Code	0	1	2	3	4	5	6	7	8	9	10	11	12
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Code	13	14	15	16	17	18	19	20	21	22	23	24	25

Substitutions & transpositions

- Two simple forms of encryption:
  - **Substitutions**
    - in which one letter is exchanged for another
  - **Transpositions**
    - in which the order of the letters is rearranged

Substitutions: The Caesar Cipher

- The Caesar Cipher
- Each letter is translated to the letter a fixed number of places after it in the alphabet.
- Caesar used a shift of 3, so plaintext letter p_i was enciphered as ciphertext letter c_i by the rule
- $c_i = E(p_i) = (p_i + 3) \bmod (26)$
- In the general form, using K as a key

  $c_i = E(p_i) = (p_i + k) \bmod (26)$

  $p_i = D(c_i) = (c_i - k) \bmod (26)$
- Example:
  - INFO SECURITY → ?

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

Substitutions: The Caesar Cipher

- Cyphertext: wklv phvvdjh lv qrw wrr kdug wr euhdn
- Cryptanalysis:
  - Blank is translated to itself?
  - How about English small words? (digrams and trigrams)
    - am, is, to, be, he, we, and, are, you, she, and so on
  - Any clue in the repeated r of wrr?
    - Xyy: see, too, odd, add
      - wklv phvvdjh lv qrw wrr kdug wr euhdn
      - T--- ------- -- -OT TOO ---- TO -----
    - How about OT?
      - Could be got, dot, hot, etc.

KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrcp	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

Figure 2.3 Brute-Force Cryptanalysis of Caesar Cipher

To be continued next lecture!

- Other symmetric cryptography
- Asymmetric cryptography