Lecture 4.1
Symmetric Ciphers

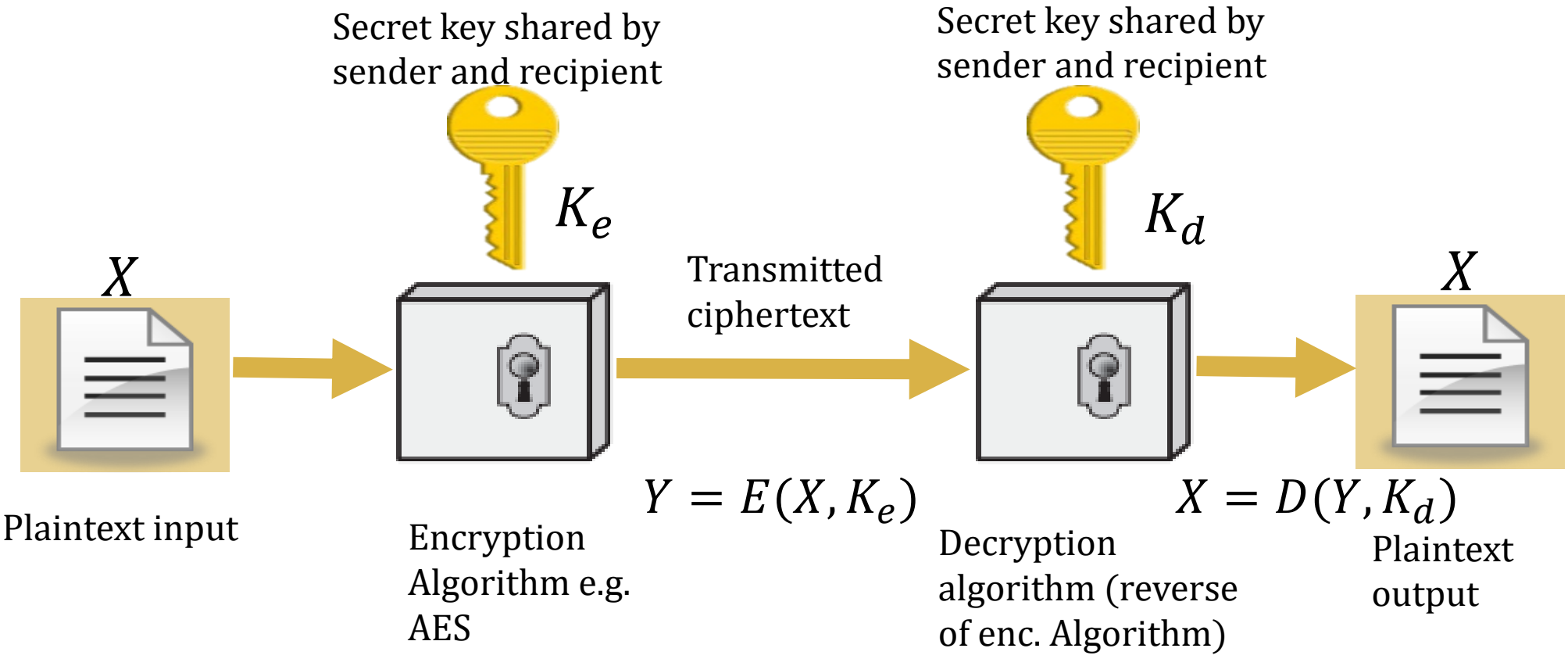
Lecture Outline

Classical Ciphers

- Classical encryption techniques
- Symmetric cipher model
- Substitution techniques
- Transposition techniques

Symmetric Key Techniques

- A Secret Key cryptosystem: decryption and encryption use the same key



Symmetric Cipher Model

A symmetric encryption scheme has five components

1. **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
2. **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
3. **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

Symmetric Cipher Model

A symmetric encryption scheme has five components

4. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
5. **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Symmetric Cipher Model

There are two requirements for secure use of conventional encryption:

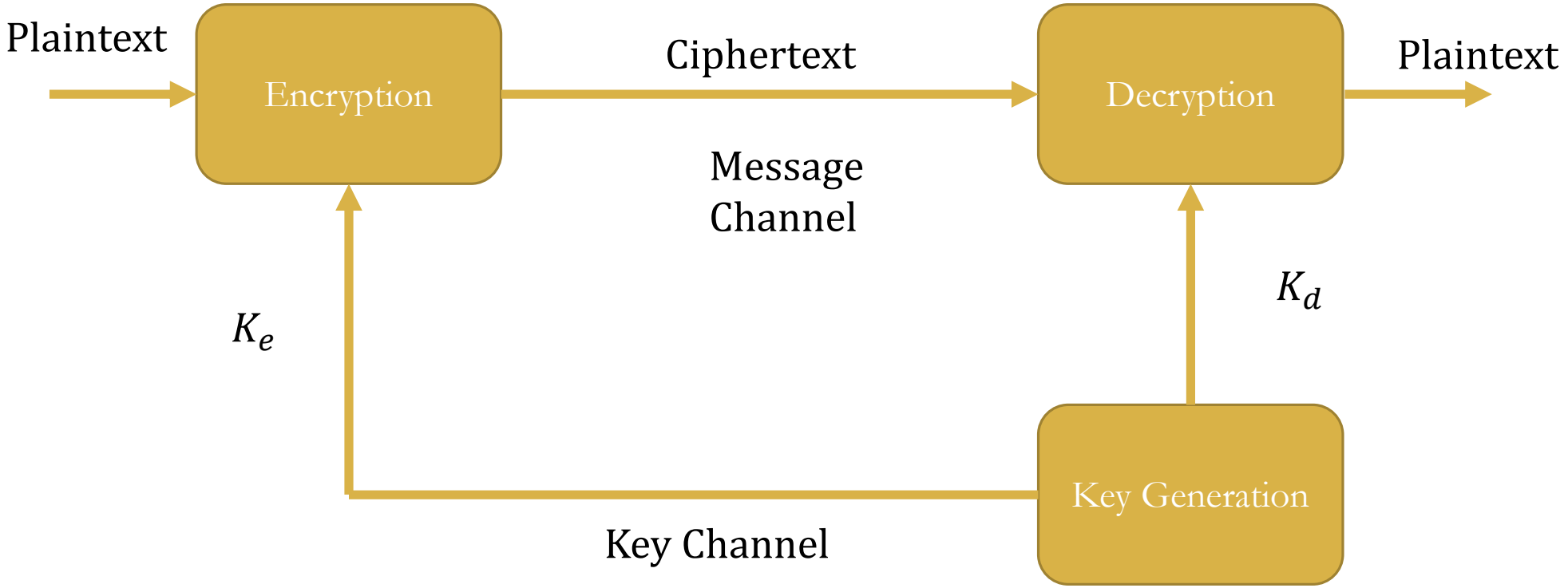
1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key.

"The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext".

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

Symmetric Key Techniques

- A Secret Key cryptosystem: decryption and encryption use the same key



- Secret key cryptosystem: $K_e = k_d$ *key channel e.g. Courier*
- Public key cryptosystem: $K_e \neq k_d$ *key channel e.g. Directory*

Properties of a good Cryptosystem

These are based on Shannon and Kirchhoff's principles

- The algorithms $\mathcal{E}$ and D contain no components or design parts which are secret
- $\mathcal{E}$ distributes meaningful messages uniformly over the entire ciphertext message space
- With the correct key $\mathcal{E}$ and D are efficient
- Without the correct key $\mathcal{E}$ and D are inefficient

Substitution Ciphers

- The encryption algorithm $\mathcal{E}k_e\ (m)$ is a substitution function which replaces *each* m ∈ $\mathcal{M}$ with the corresponding c ∈ C with the substitution function being parameterized by a secret key. The decryption $Dk_d\ (c)$ is merely reverse substitution
- Examples include:

1. Simple substitution cipher
2. Polyalphabetic ciphers
3. The Vernam and one time pad

Substitution Ciphers

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

Simple Substitution Ciphers: Ceasar

One of the earliest substitution ciphers.

- Ceasar cipher: Where each character is shifted three places up i.e. A becomes D, B becomes E, etc. Here, $K = \mathcal{M} = \mathbb{C}$
- Example

Plaintext	V	O	Y	A	G	E	R
Key	+3	+3	+3	+3	+3	+3	+3
Cipher	Y	R	B	D	J	H	U

- A more complex substitution cipher would be created if instead of incrementing each character by three, we use a more complex key e.g. a key of "123"
- Alternatively, we can have each letter of the alphabet correspond to a different letter of the alphabet without a set pattern (randomly)

Simple Substitution Ciphers: Ceasar Cipher

- In shift ciphers, $|K| = |\mathcal{M}| = |\mathrm{C}|$, let N= $\# \mathcal{M}$
- The encryption and decryption mappings are defined by:

$$E_k(m) \leftarrow m + k(mod\ N)$$
$$D_k(c) \leftarrow c - k(mod\ N)$$

$where\, m, c, k \in \mathbb{Z}_N$

- If the gcd(k, N) = 1, then $\forall_{m<N}: km(mod\ N)$ ranges over the entire message space $\mathbb{Z}_N$. For such a k and m, c < N
- Under multiplication

$$E_k(m) \leftarrow km(mod\ N)$$
$$D_k(c) \leftarrow k^{-1}c(mod\ N)$$

} is also a simple substitution cipher

Simple Substitution Ciphers: Affine Cipher

- Similarly $k_1 m + k_2 (mod\ N)$ also defines a simple substitution cipher called the Affine cipher

$$E_k(m) \leftarrow k_1 m + k_2 (mod\ N)$$
$$D_k(c) \leftarrow k^{-1}(c - k_2)(mod\ N)$$

Affine Cipher

Simple Substitution Ciphers: Affine Cipher

- Here the letters of an alphabet of size m are first mapped to the integers in the range $0, \ldots\ldots, m-1$. It then uses modular arithmetic to transform the integer that each plain text letter corresponds to another integer that corresponds to a ciphertext letter.
- Encryption

$$E_k(m) \leftarrow k_1 m + k_2 \, (mod \, \mathrm{N})$$

- The modulus N is the size of the alphabet and k_1, k_2 are the keys of the cipher. The value k_1 must be chosen such that k_1 and m are coprime $(\gcd(k_1, m) = 1)$

Simple Substitution Ciphers: Affine Cipher

- Decryption

$$D_k(c) \leftarrow k^{-1}(c - k_2)(mod\ N)$$

where k_1^{-1} is the modular multiplicative inverse of k_1 modulo N i.e. k_1^{-1} mod N

- The multiplicative inverse of k_1 exists if k_1 and m are coprime and hence it can be shown that the decryption function is the inverse of the encryption function: $c \leftarrow E_k(m) \leftarrow k_1 m + k_2(mod\ N)$

$$D_k(c) \leftarrow k_1^{-1}(c - k_2)(mod\ N)$$
$$= k_1^{-1}(((k_1 m + k_2) mod\ N) - k_2(mod\ N)$$
$$= k_1^{-1}(k_1 m + k_2 - k_2)(mod\ N)$$
$$= k_1^{-1} k_1 m(mod\ N)$$
$$= m(mod\ N)$$
$$= m$$

Simple Substitution Ciphers

Disadvantages of Mono-alphabetic ciphers

- If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed:

Simply try all the 25 possible keys.

Three important characteristics of this problem that allow for the use of a brute force cryptanalysis are:

1. The encryption and decryption algorithms are known.

2. There are only 25 keys to try.

3. The language of the plaintext is known and easily recognizable.

Simple Substitution Ciphers

Disadvantages of Mono-alphabetic ciphers

Note: The key is a number from 0 to 25

Breaking the Ceasar Cipher

- Caesar can be broken if we only know one pair (plain letter, encrypted letter)
  - The difference between them is the key
- Caesar can be broken even if we only have the encrypted text and

no knowledge of the plaintext

  - Brute-force attack is easy: *there are only 25 keys possible*
  - Try all 25 keys and check to see which key gives an intelligible message

Simple Substitution Ciphers

```
          PHHW PH DIWHU WKH WRJD SDUWB
KEY
    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
```

Why is Caesar easy to break?

- Only 25 keys to try
- The language of the plaintext is known and easily recognizable

1. What if the language is unknown?
2. What if the plaintext is a binary file of an unknown format?

Polyalphabetic Ciphers

- Another major disadvantage of the mono-alphabetic ciphers is that they are vulnerable to frequency attacks.
- A substitution cipher is called a polyalphabetic cipher if a plaintext message element in P maybe substituted into many/any ciphertext message element in C.

Example Vigenere cipher

Key string = GOLD (6,14,11,3)

Plaintext = proceed meeting as agreed

Ciphertext = vfzfkso pkseltu lv guchkr

$$C_i \equiv (P_i + K_i) \pmod{26}$$

$$P_i \equiv (C_i - K_i) \pmod{26}$$

Polyalphabetic Ciphers

- 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
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

15	17	14	2	4	4	3	12	4	4	19	8	13	6	0	18	0	6	17	4	4	3
6	14	11	3	6	14	11	3	6	14	11	3	6	14	11	3	6	14	11	3	6	14
21	5	25	5	10	18	14	15	10	18	4	11	19	20	11	21	6	20	2	7	10	17

Polyalphabetic Ciphers

- 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
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

Vernam Cipher and One Time Pad

- Vernam proposed a bit-wise exclusive OR ($\oplus$)of the message stream with a truly random zero-one (0,1) stream which was shared by the sender and recipient.
- It carries out addition modulo 2
- The message is assumed to be a string of n binary bits

$$M = b_1 b_2 \dots b_n \in \{0,1\}^n$$

The key is also assumed to be a string of n binary bits

$$K = k_1 k_2 \dots k_n \in \{0,1\}^n$$

- Encryption takes place one bit at a time and the cipher text

$C = c_1 c_2 \dots c_n \in \{0,1\}^n$ is found by XORing each message bit with the corresponding key bit.

$$c = b_1 \oplus k_1$$

Vernam Cipher and One Time Pad

Example

- SENDING

Message	0	0	1	0	1	1	0	1	0
XOR	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Pad	1	0	0	1	1	1	0	0	1
Cipher	1	0	1	1	0	0	0	1	1

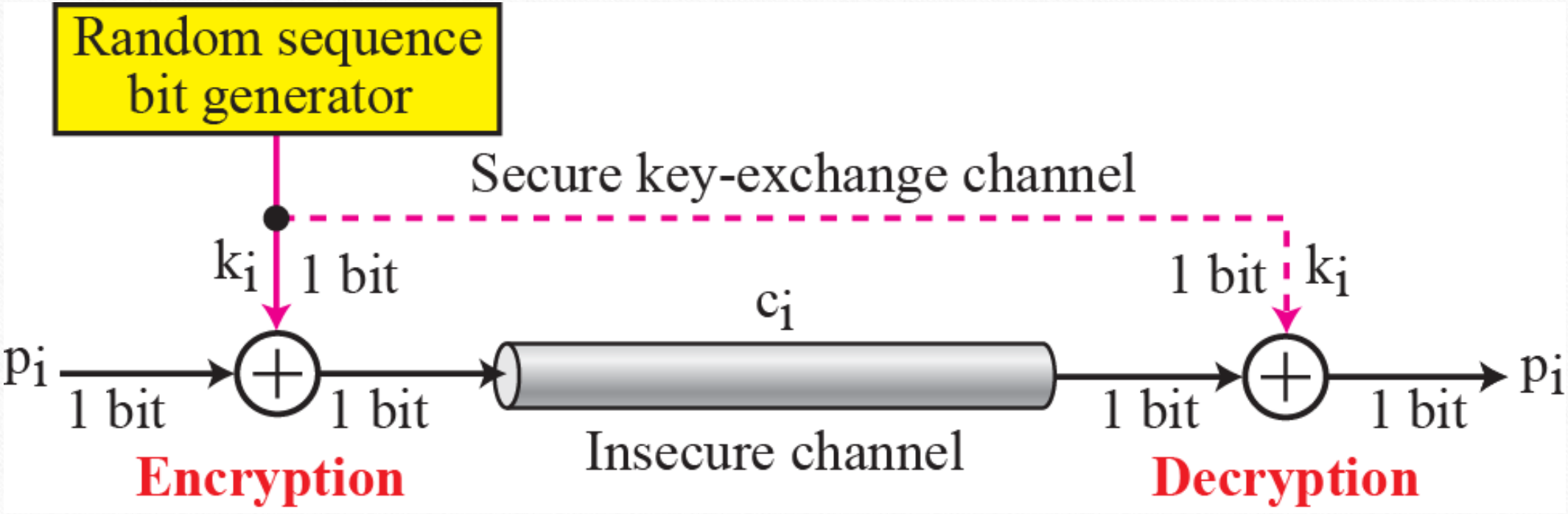
- RECEIVING

Cipher	1	0	1	1	0	0	0	1	1
XOR	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Pad	1	0	0	1	1	1	0	0	1
Message	0	0	1	0	1	1	0	1	0

One Time Pad

- Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated.
- In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded.
- Each new message requires a new key of the same length as the new message.
- Such a scheme, known as a **one-time pad,** is unbreakable.
- It produces random output that bears no statistical relationship to the plaintext.
- Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.

One Time Pad


Random sequence bit generator
Secure key-exchange channel
ki
1 bit
ci
1 bit
ki
pi
1 bit
1 bit
1 bit
1 bit
pi
Insecure channel
Encryption
Decryption

One Time Pad

Example

ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

We now show two different decryptions using two different keys:

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key: pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
plaintext: mr mustard with the candlestick in the hall

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key: mfugpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt
plaintext: miss scarlet with the knife in the library

Transposition Ciphers

- Transforms a message by rearranging the position of the elements in the message without changing the identities of the message.
- This ciphers encrypt the plaintext by moving small pieces of the message around such that the letters all stay the same but the order is mixed up.
- Example:

V	O	Y	A	G	E	R
O	V	A	Y	E	G	R

- This rep. a primitive transposition where every two letters are switched with each other.
- A plaintext message block can be transposition enciphered to b! possible cipher-texts (permutations)

Transposition Cipher

- Another simplest of such cipher is the **rail fence** technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- For example, to encipher the message "meet me after the toga party" with a rail fence of depth 2, we write the following:

```
m e m a t r h t g p r y
  e t e f e t e o a a t
```

- The encrypted message is

MEMATRHTGPRYETEFETEOAAT

Transposition Cipher

- This sort of thing would be trivial to cryptanalyze.
- A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.
- The order of the columns then becomes the key to the algorithm.
- For example,

Key	4	3	1	2	5	6	7
Plaintext	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Transposition Cipher

- Thus, in this example, the key is 4312567.
- To encrypt, start with the column that is labeled 1, in this case column 3.
- Write down all the letters in that column.
- Proceed to column 4, which is labeled 2, then column 2, then column 1, then columns 5, 6, and 7.

Transposition Cipher

- A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.
- For the type of columnar transposition just shown, cryptanalysis is fairly straightforward and involves laying out the ciphertext in a matrix and playing around with column positions.
- Digram and trigram frequency tables can be useful.
- The transposition cipher can be made significantly more secure by performing more than one stage of transposition.
- The result is a more complex permutation that is not easily reconstructed. Thus, if the foregoing message is re-encrypted using the same algorithm

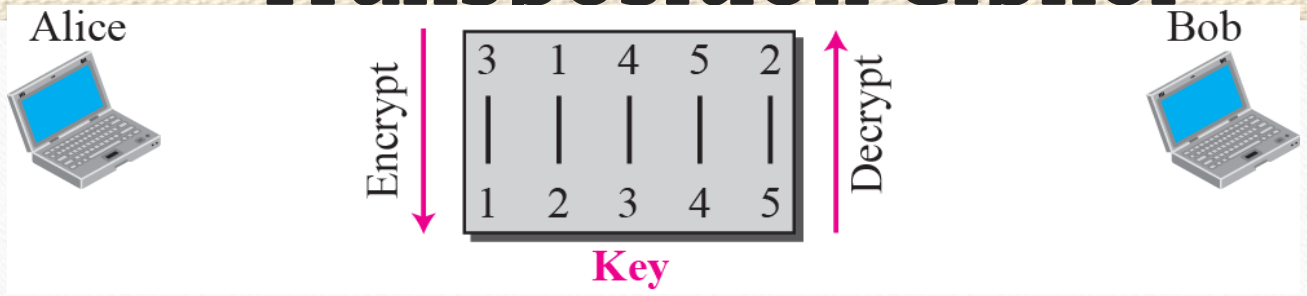
Transposition Cipher

Key	4	3	1	2	5	6	7
Plaintext	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	i	x	k
	n	l	y	p	e	t	z

Ciphertext: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

Double transposition

Transposition Cipher



Plaintext

e n e m y a t t a c k s t o n i g h t z

Write row by row

e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	Z	G

Read column by column

E T T H E A K I M A O T Y C N Z N T S G

Ciphertext

Transmission

Plaintext

e n e m y a t t a c k s t o n i g h t z

Read row by row

e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	Z	G

Write column by column

E T T H E A K I M A O T Y C N Z N T S G

Ciphertext

Classical Ciphers: Usefulness and Security

- The two working principles of classical ciphers is : substitution and transposition.
- Modern symmetric encryption algorithms use combinations of substitution and transposition e.g. DES, AES.
- For the secure use of classical ciphers, the following conditions are necessary

1. $|K| \geq |M|$
2. k $\in {}_{u}K$ and its used once in each encryption

- They can be used to construct zero knowledge proofs which allow a prover (Alice) to show a verifier (Bob) that's she knows the pre-image f(z) (which is z<n) without disclosing to the latter the pre-image.

Classical Ciphers: Substitution & Permutation

- Claude Shannon observed that there are two fundamental techniques for encryption:

1. Confusion – Obscuring the relationship between the plaintext and the ciphertext
2. Diffusion – Spreading the change throughout the ciphertext

- The simplest form of confusion is substitution: replacing one symbol by another.
- The simplest form of diffusion is permutation: moving the symbols of a block around.
- Frequency analysis can be used to break both.
- Nevertheless, combinations of these operations form the backbone of modern cryptosystems