Course: Cryptography and Network Security
Code: CS-34310
Branch: M.C.A - 4th Semester

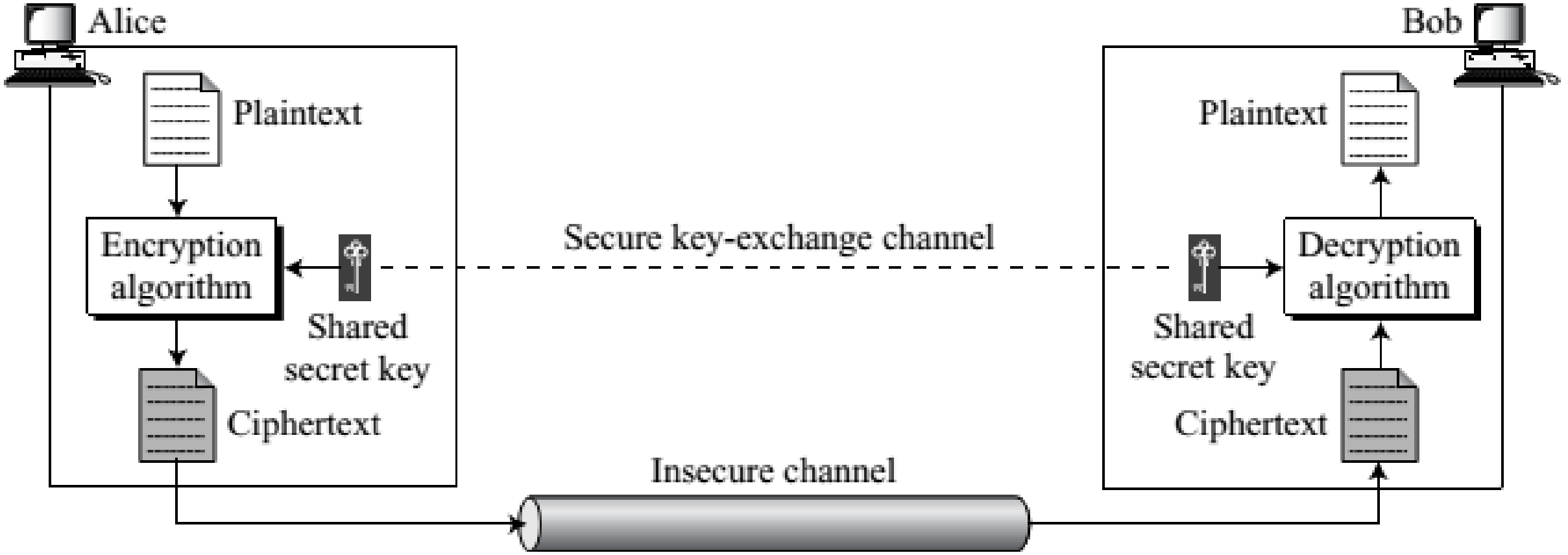
Lecture – 5b: Symmetric-Key Ciphers

Faculty & Coordinator : Dr. J Sathish Kumar (JSK)

Department of Computer Science and Engineering

Motilal Nehru National Institute of Technology Allahabad,
Prayagraj-211004

Symmetric-key Cipher



Symmetric-key Cipher

- Symmetric-key encipherment uses a single key for both encryption and decryption.
- Encryption and decryption algorithms are inverses of each other.
- If P is the plaintext, C is the ciphertext, and K is the key, the encryption algorithm $E_k(x)$ creates the ciphertext from the plaintext; the decryption algorithm $D_k(x)$ creates the plaintext from the ciphertext.
- We assume that $E_k(x)$ and $D_k(x)$ are inverses of each other: they cancel the effect of each other if they are applied one after the other on the same input.

Encryption: $C = E_k(P)$ Decryption: $P = D_k(C)$

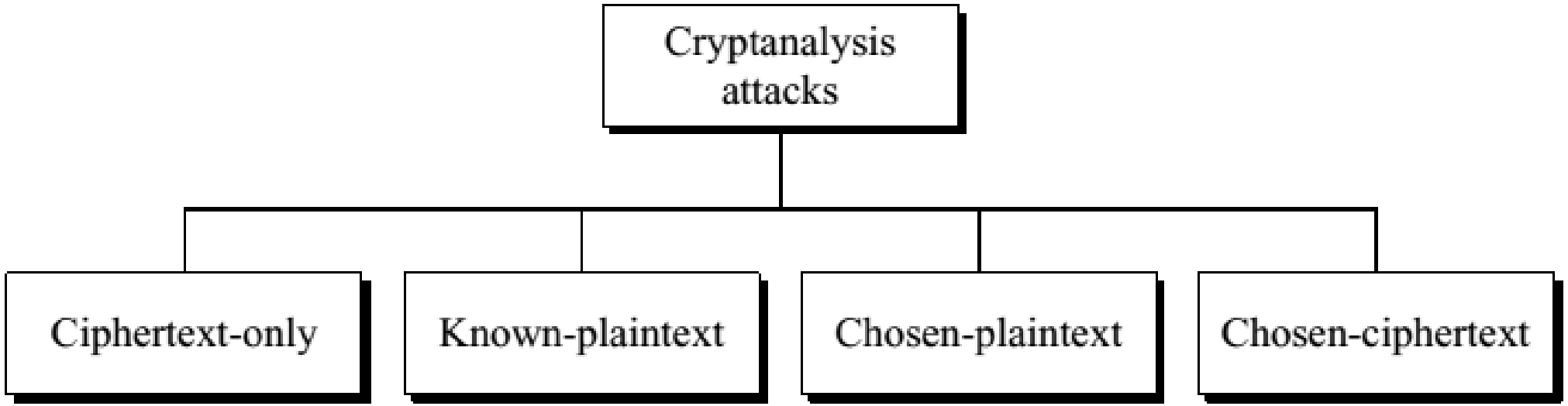
In which, $D_k(E_k(x)) = E_k(D_k(x)) = x$

Alice: $C = E_k(P)$ **Bob:** $P_1 = D_k(C) = D_k(E_k(P)) = P$

Kerckhoff’s Principle

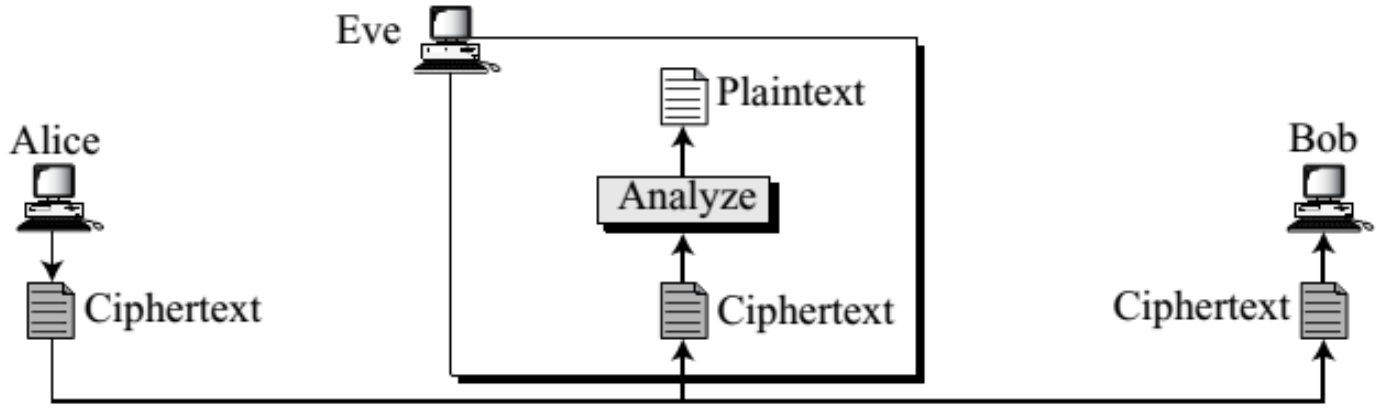
- Although it may appear that a cipher would be more secure if we hide both the encryption/decryption algorithm and the secret key, this is not recommended.
- Based on Kerckhoff’s principle, one should always assume that the adversary, Eve, knows the encryption/decryption algorithm.
- The resistance of the cipher to attack must be based only on the secrecy of the key.
- In other words, guessing the key should be so difficult that there is no need to hide the encryption/decryption algorithm.
- This principle manifests itself more clearly when we study modern ciphers.
- There are only a few algorithms for modern ciphers today.
- The key domain for each algorithm, however, is so large that it makes it difficult for the adversary to find the key.

Cryptanalysis



Ciphertext-Only Attack

- In a ciphertext-only attack, Eve has access to only some ciphertext.
- She tries to find the corresponding key and the plaintext.
- The assumption is that Eve knows the algorithm and can intercept the ciphertext.
- The ciphertext-only attack is the most probable one because Eve needs only the ciphertext for this attack.
- To thwart the decryption of a message by an adversary, a cipher must be very resisting to this type of attack.

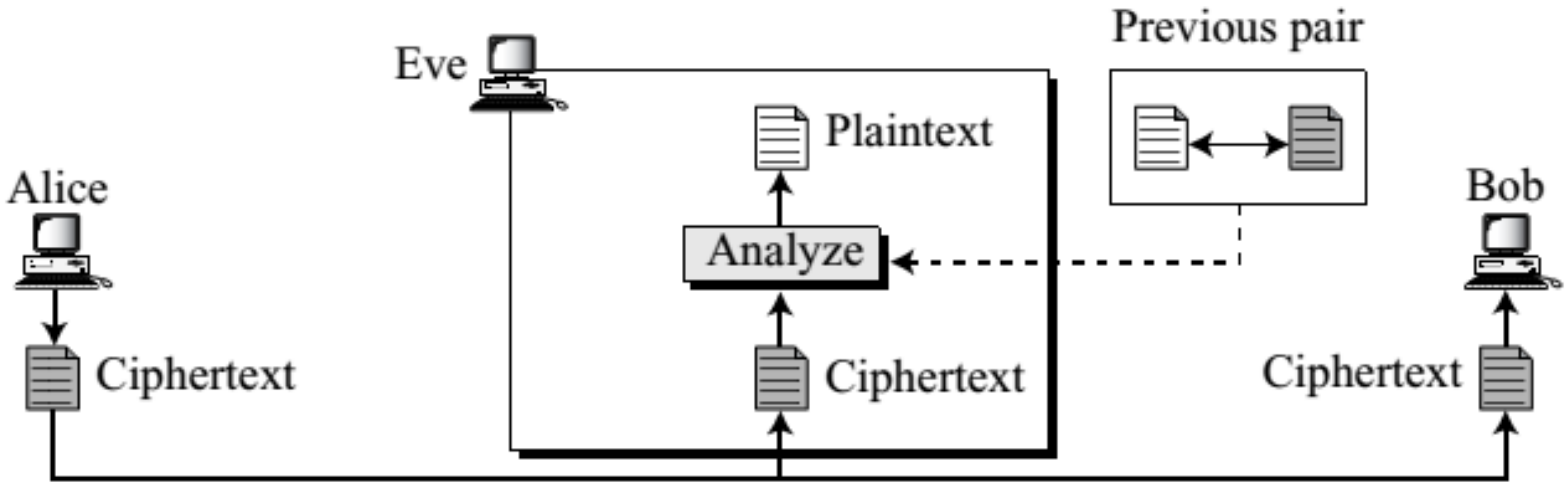


Ciphertext-Only Attack

- Brute-Force Attack
  - In the brute-force method or exhaustive-key-search method, Eve tries to use all possible keys.
  - We assume that Eve knows the algorithm and knows the key domain (the list of all possible keys).
  - Using the intercepted cipher, Eve decrypts the ciphertext with every possible key until the plaintext makes sense.
  - Using brute-force attack was a difficult task in the past; it is easier today using a computer.
  - To prevent this type of attack, the number of possible keys must be very large.
- Statistical Attack
  - The cryptanalyst can benefit from some inherent characteristics of the plaintext language to launch a statistical attack.
  - For example, we know that the letter E is the most frequently used letter in English text.
  - The cryptanalyst finds the mostly-used character in the ciphertext and assumes that the corresponding plaintext character is E.
  - After finding a few pairs, the analyst can find the key and use it to decrypt the message.
  - To prevent this type of attack, the cipher should hide the characteristics of the language.
- Pattern Attack
  - Some ciphers may hide the characteristics of the language, but may create some patterns in the ciphertext.
  - A cryptanalyst may use a pattern attack to break the cipher.
  - Therefore, it is important to use ciphers that make the ciphertext look as random as possible.

Known-Plaintext Attack

- In a known-plaintext attack, Eve has access to some plaintext/ciphertext pairs in addition to the intercepted ciphertext that she wants to break.

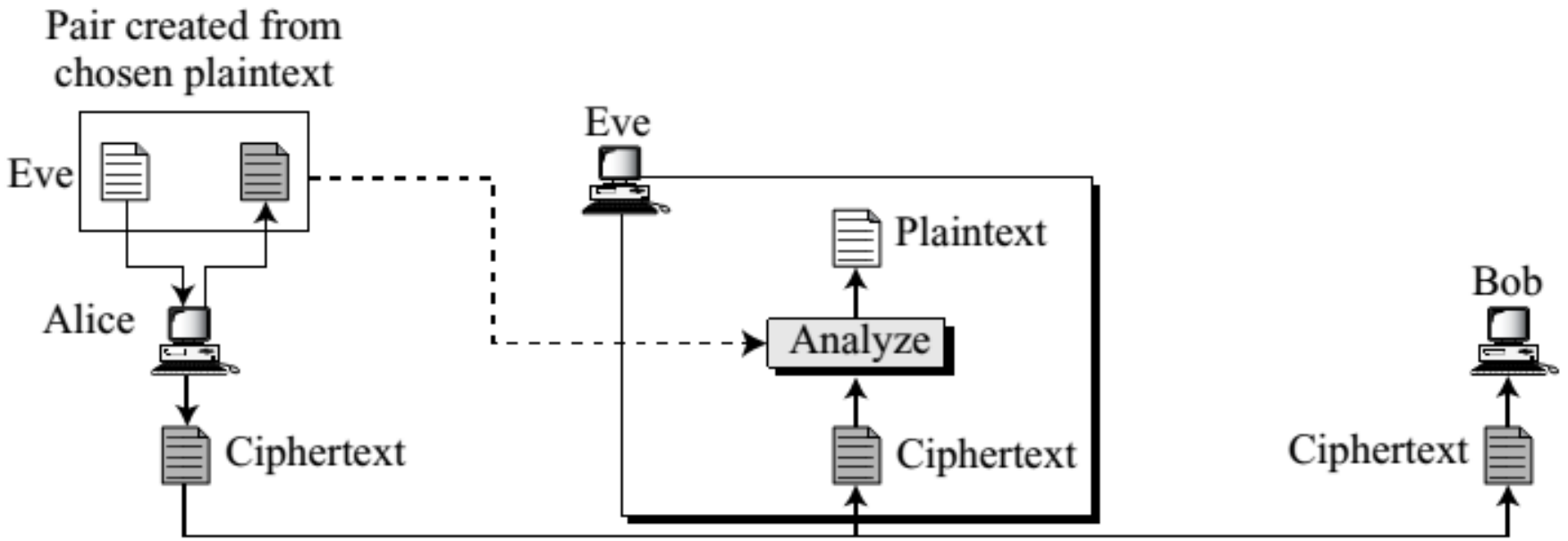


Known-Plaintext Attack

- The plaintext/ciphertext pairs have been collected earlier.
- For example, Alice has sent a secret message to Bob, but she has later made the contents of the message public.
- Eve has kept both the ciphertext and the plaintext to use them to break the next secret message from Alice to Bob, assuming that Alice has not changed her key.
- Eve uses the relationship between the previous pair to analyze the current ciphertext.
- The same methods used in a ciphertext-only attack can be applied here.
- This attack is easier to implement because Eve has more information to use for analysis.
- However, it is less likely to happen because Alice may have changed her key or may have not disclosed the contents of any previous messages.

Chosen-Plaintext Attack

- The chosen-plaintext attack is similar to the known-plaintext attack, but the plaintext/ciphertext pairs have been chosen by the attacker herself.

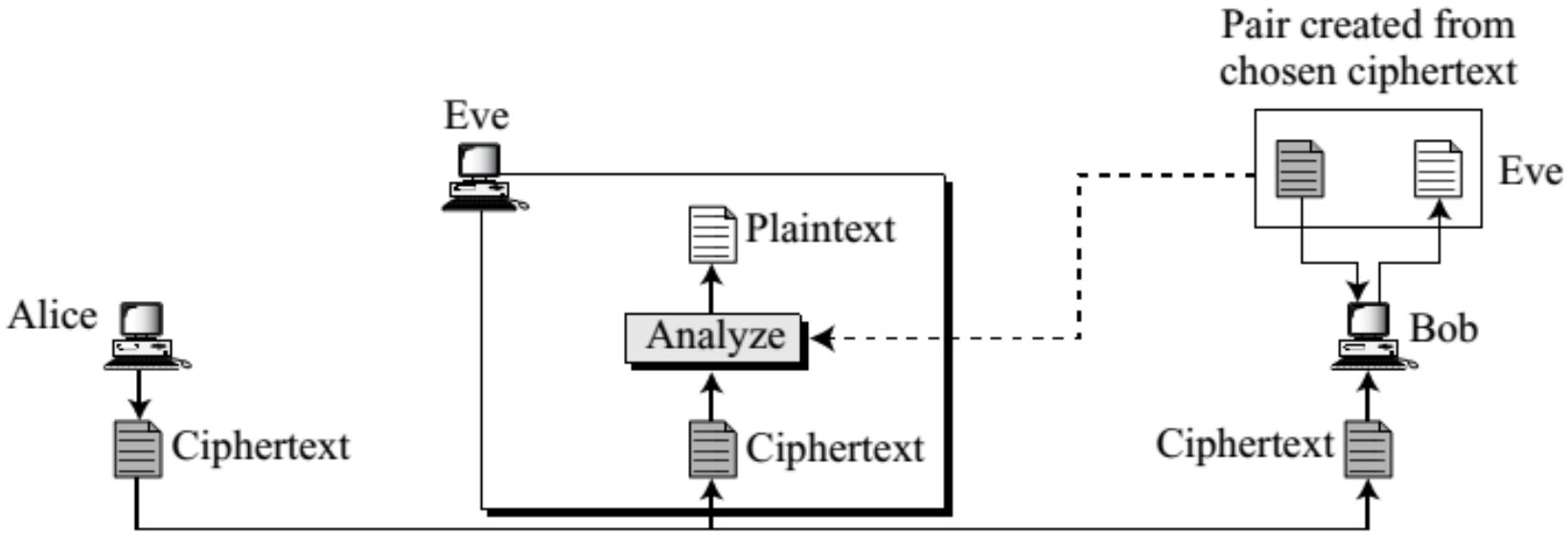


Chosen-Plaintext Attack

- This can happen, for example, if Eve has access to Alice's computer.
- She can choose some plaintext and intercept the created ciphertext.
- Of course, she does not have the key because the key is normally embedded in the software used by the sender.
- This type of attack is much easier to implement, but it is much less likely to happen.

Chosen-Ciphertext Attack

- The chosen-ciphertext attack is similar to the chosen-plaintext attack, except that Eve chooses some ciphertext and decrypts it to form a ciphertext/plaintext pair.
- This can happen if Eve has access to Bob's computer.



Categories of Traditional Ciphers

- Substitution ciphers and Transposition ciphers.
- In a substitution cipher, we replace one symbol in the ciphertext with another symbol.
- In a transposition cipher, we reorder the position of symbols in the plaintext.

SUBSTITUTION CIPHERS

- A substitution cipher replaces one symbol with another.
- Monoalphabetic Ciphers
  - In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.
  -

Plaintext: hello **Ciphertext:** KHOOR

Plaintext: hello **Ciphertext:** ABNZF

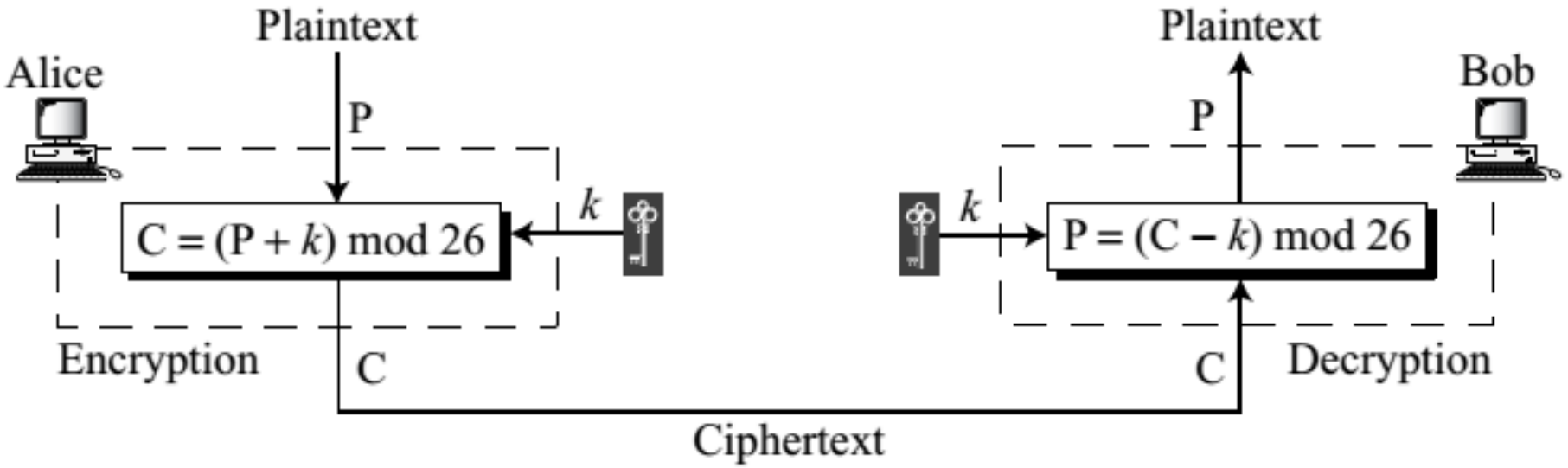
Additive Cipher

- This cipher is sometimes called a shift cipher and sometimes a Caesar cipher, but the term additive cipher better reveals its mathematical nature.
- When the cipher is additive, the plaintext, ciphertext, and key are integers in Z_{26}.

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 →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Representation of plaintext and ciphertext characters in Z_{26}

Additive Cipher



$$P_1 = (C - k) \bmod 26 = (P + k - k) \text{ mode } 26 = P$$

Example #1:
Use the additive cipher with key = 15 to encrypt the message “hello”.
And decrypt to verify using the same key

Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

Ciphertext: W → 22	Decryption: (22 – 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 – 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 – 15) mod 26	Plaintext: 14 → o

- Additive ciphers are vulnerable to ciphertext-only attacks using exhaustive key searches (brute-force attacks).
- The key domain of the additive cipher is very small;there are only 26 keys.
- However, one of the keys, zero, is useless (the ciphertext is the same as the plaintext).
- This leaves only 25 possible keys.
- Eve can easily launch a bruteforce attack on the ciphertext.

s

Example #2

Eve has intercepted the ciphertext “UVACLYFZLJBYL”. Show how she can use a brute-force attack to break the cipher.

Ciphertext: UVACLYFZLJBYL

K = 1	→	**Plaintext:** tuzbkxeykiaxk
K = 2	→	**Plaintext:** styajwdxjhzwj
K = 3	→	**Plaintext:** rsxzivcwigyvi
K = 4	→	**Plaintext:** qrwyhubvhfxuh
K = 5	→	**Plaintext:** pqvxgtaugewtg
K = 6	→	**Plaintext:** opuwfsztfdvsf
K = 7	→	**Plaintext:** notverysecure

Cryptanalysis

- Additive ciphers are also subject to statistical attacks. This is especially true if the adversary has a long ciphertext.
- The adversary can use the frequency of occurrence of characters for a particular language.

Letter	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Cryptanalysis

Digram	TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
Trigram	THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

The most common two-letter groups (digrams) and three-letter groups (trigrams) for the English text are shown in Table

Example #3

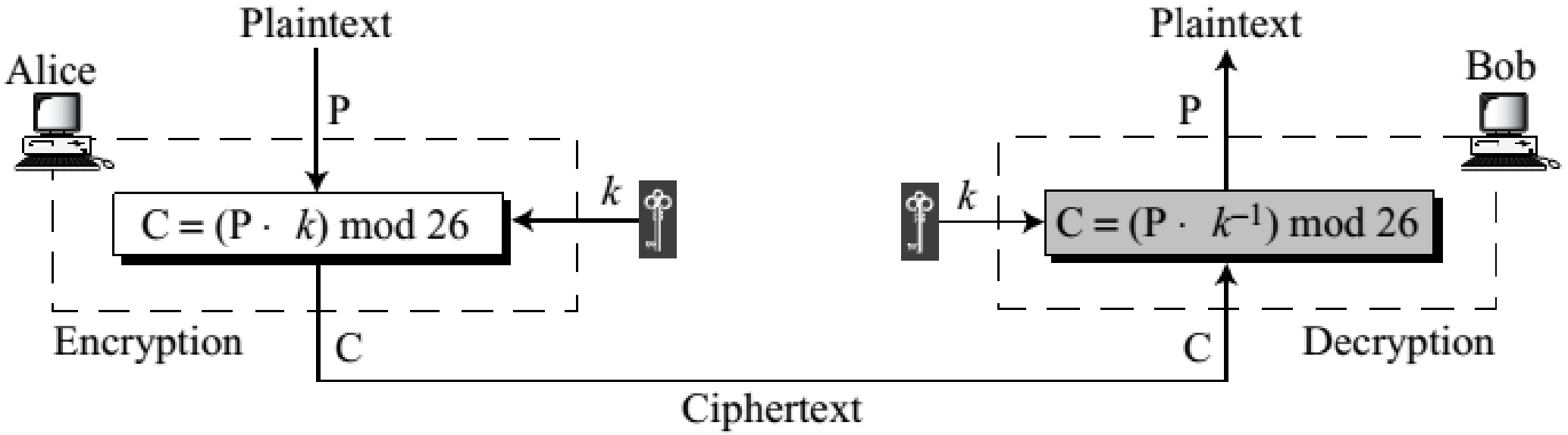
- Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-
VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

- When Eve tabulates the frequency of letters in this ciphertext, she gets: I =14, V =13, S =12, and so on.
- The most common character is I with 14 occurrences.
- This shows that character I in the ciphertext probably corresponds to the character e in plaintext. This means key = 4. Eve deciphers the text to get

the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

Multiplicative Ciphers



In a multiplicative cipher, the plaintext and ciphertext are integers in Z26; The key is an integer in Z26*.

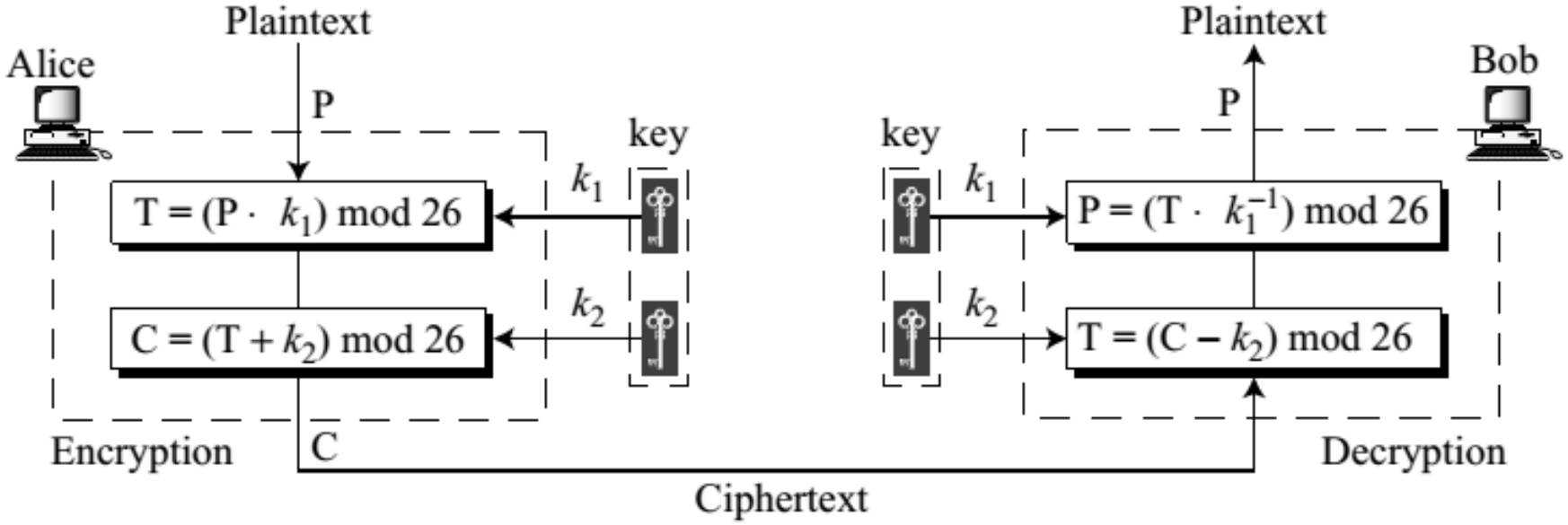
Multiplicative Ciphers

- What is the key domain for any multiplicative cipher?
  - The key needs to be in Z_{26}*. This set has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21,23, 25.
- We use a multiplicative cipher to encrypt the message “hello” with a key of 7.

Plaintext: h $\rightarrow$ 07	Encryption: $(07 \times 07) \bmod 26$	ciphertext: 23 $\rightarrow$ X
Plaintext: e $\rightarrow$ 04	Encryption: $(04 \times 07) \bmod 26$	ciphertext: 02 $\rightarrow$ C
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: l $\rightarrow$ 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow$ Z
Plaintext: o $\rightarrow$ 14	Encryption: $(14 \times 07) \bmod 26$	ciphertext: 20 $\rightarrow$ U

Affine Cipher

- Combine the additive and multiplicative ciphers to get what is called the affine cipher-a combination of both ciphers with a pair of keys.
- The first key is used with the multiplicative cipher; the second key is used with the additive cipher.



Affine Cipher

$$C = (P \times k_1 + k_2) \bmod 26 \qquad P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

where k_1^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2

Use an affine cipher to encrypt the message “hello” with the key pair (7, 2).

P: h → 07	Encryption: $(07 \times 7 + 2) \bmod 26$	C: 25 → Z
P: e → 04	Encryption: $(04 \times 7 + 2) \bmod 26$	C: 04 → E
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: l → 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 → B
P: o → 14	Encryption: $(14 \times 7 + 2) \bmod 26$	C: 22 → W

Affine Cipher

- Use the affine cipher to decrypt the message “ZEBBW” with the key pair (7, 2) in modulus 26.
- Add the additive inverse of −2 ≡ 24 (mod 26) to the received ciphertext.
- Then multiply the result by the multiplicative inverse of $7^{-1} \equiv 15 \pmod{26}$ to find the plaintext characters.
- Because 2 has an additive inverse in Z_{26} and 7 has a multiplicative inverse in Z_{26}^*

C: Z → 25	Decryption: $((25 - 2) \times 7^{-1}) \bmod 26$	P:07 → h
C: E → 04	Decryption: $((04 - 2) \times 7^{-1}) \bmod 26$	P:04 → e
C: B → 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 → l
C: B → 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 → l
C: W → 22	Decryption: $((22 - 2) \times 7^{-1}) \bmod 26$	P:14 → o

Cryptanalysis of Affine Cipher

PWUFFOGWCHFDWIWEJOUUNJORSMDWRHVCMWJUPVCCG

Although the brute-force and statistical method of ciphertext-only attack can be used, let us try a chosen-plaintext attack.

Eve also very briefly obtains access to Alice's computer and has only enough time to type a two-letter plaintext: "et".

She then tries to encrypt the short plaintext using two different algorithms, because she is not sure which one is the affine cipher.

Algorithm 1:	Plaintext: et	ciphertext: $\rightarrow$ WC
Algorithm 2:	Plaintext: et	ciphertext: $\rightarrow$ WF

Cryptanalysis of Affine Cipher

Eve knows that if the first algorithm is affine, she can construct the following two equations based on the first data set.

e → W	04 → 22	$(04 \times k_1 + k_2) \equiv 22 \pmod{26}$
t → C	19 → 02	$(19 \times k_1 + k_2) \equiv 02 \pmod{26}$

These two congruence equations can be solved and the values of k_1 and k_2 can be found.

$$\begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 19 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 22 \\ 2 \end{bmatrix} = \begin{bmatrix} 19 & 7 \\ 3 & 24 \end{bmatrix} \begin{bmatrix} 22 \\ 2 \end{bmatrix} = \begin{bmatrix} 16 \\ 10 \end{bmatrix} \longrightarrow k_1 = 16 \quad k_2 = 10$$

However, this answer is not acceptable because $k_1 = 16$ cannot be the first part of the key. Its value, 16, does not have a multiplicative inverse in Z_{26}^*.

Cryptanalysis of Affine Cipher

Eve now tries the result of the second set of data

e → W	04 → 22	$(04 \times k_1 + k_2) \equiv 22 \pmod{26}$
t → F	19 → 05	$(19 \times k_1 + k_2) \equiv 05 \pmod{26}$

The square matrix and its inverse are the same. Now she has $k_1 = 11$ and $k_2 = 4$.
This pair is acceptable because k_1 has a multiplicative inverse in $Z_{26}*$.
She tries the pair of keys (19, 22), which are the inverse of the pair (11, 4), to decipher the message. The plaintext is

best time of the year is spring when flowers bloom