

Chapter 10 CIPHER TECHNIQUES

- **Cryptographic systems are sensitive to environment.**
- **If a cryptosystem is used in a network, it introduces many problems.**
- **The key point is that the if a cryptosystem is not implemented correctly, it may be vulnerable to attacks.**

10.1 Problems

- **The use of a cipher without consideration of the environment may not provide any security.**
 - **Three examples will make this point clear:**
 - **Precomputing the possible messages**
 - Cathy knows that Alice will send one of 2 messages.
 - The uncertainty is which one Alice will send.
 - Cathy enciphers both messages with Bob's public key.
 - When Alice sends the message, Cathy intercepts and compares it with the two she has computed.
 - Therefore, Cathy knows the message sent by Alice.

Chapter 10 CIPHER TECHNIQUES

- **Misordered blocks**
 - In certain cases, parts of a message can be deleted, replayed, or reordered.
 - **EXAMPLE: Consider RSA.**
 - » Choose $p=7$ and $q=11 \Rightarrow n=77$ and $\phi(n)=60$.
 - » Bob chooses $e=7 \Rightarrow$ his private key $d=53$.
 - » In this cryptosystem, each plaintext character is represented by a number from 00(A) to 25(Z). 26 represents the blank character.
 - » Alice wants to send Bob the message LIVE (11 08 21 04).
 - » She enciphers each character of the message using Bob's public key $e=7$: 44 57 21 16.
 - » Cathy intercepts it and rearranges the ciphertext: 16 21 57 44.
 - » Bob decipheres the message to read EVIL.
 - » Even if each character is digitally signed by Alice, Bob cannot detect this attack.
 - » One solution for Alice is to generate a cryptographic checksum of the entire message, and sign that value.
- **Statistical regularities**
 - If each part of a message is enciphered separately, the same plaintext will always produce the same ciphertext.
 - This type of encipherment is called code book mode.
 - Each party looks up in a list of plaintext-ciphertext pairs.
 - Plaintext: 3231 3433 3635 3837 3231 3433 3635 3837
 - Ciphertext: ef7c 4bb2 b4ce 6f3b ef7c 4bb2 b4ce 6f3b

Chapter 10 CIPHER TECHNIQUES

10.2 Stream and Block Ciphers

- ***E* encipherment function**
 - $E_k(b)$ encipherment of message b with key k
 - $m = b_1b_2 \dots$, where each b_i is of a fixed length
- **Block cipher**
 - $E_k(m) = E_k(b_1)E_k(b_2) \dots$
 - The DES is a block cipher. Each message is broken into 64-bit blocks and the same 56-bit key is used to encipher each block.
- **Stream cipher**
 - $k = k_1k_2 \dots$
 - $E_k(m) = E_{k_1}(b_1)E_{k_2}(b_2) \dots$
 - If $k_1k_2 \dots$ repeats itself, the cipher is periodic and the length of its period is one cycle of $k_1k_2 \dots$
 - The Vigenere cipher is a stream cipher.
 - This is a periodic cipher because the key is of finite length.
 - b_i is a character of the message and k_i is a character of the key.
 - The one-time pad is also a stream cipher but it is not periodic.

Chapter 10 CIPHER TECHNIQUES

- Stream Ciphers

- There are two types of stream ciphers:
synchronous and self-synchronous.
- Bit-oriented stream ciphers implement the one-time pad by xoring each bit of the key with one bit of the message.
- Example: $m = 00101, k = 10010 \Rightarrow c = 10111$.
- How can one generate a random, infinitely long key?

- Synchronous Stream Ciphers

- To generate a random, infinitely long key, synchronous stream ciphers generate bits from a source other than the message itself.
- The simplest synchronous stream cipher extracts bits from a register.
 - The contents of the register change on the basis of the current contents of the register.

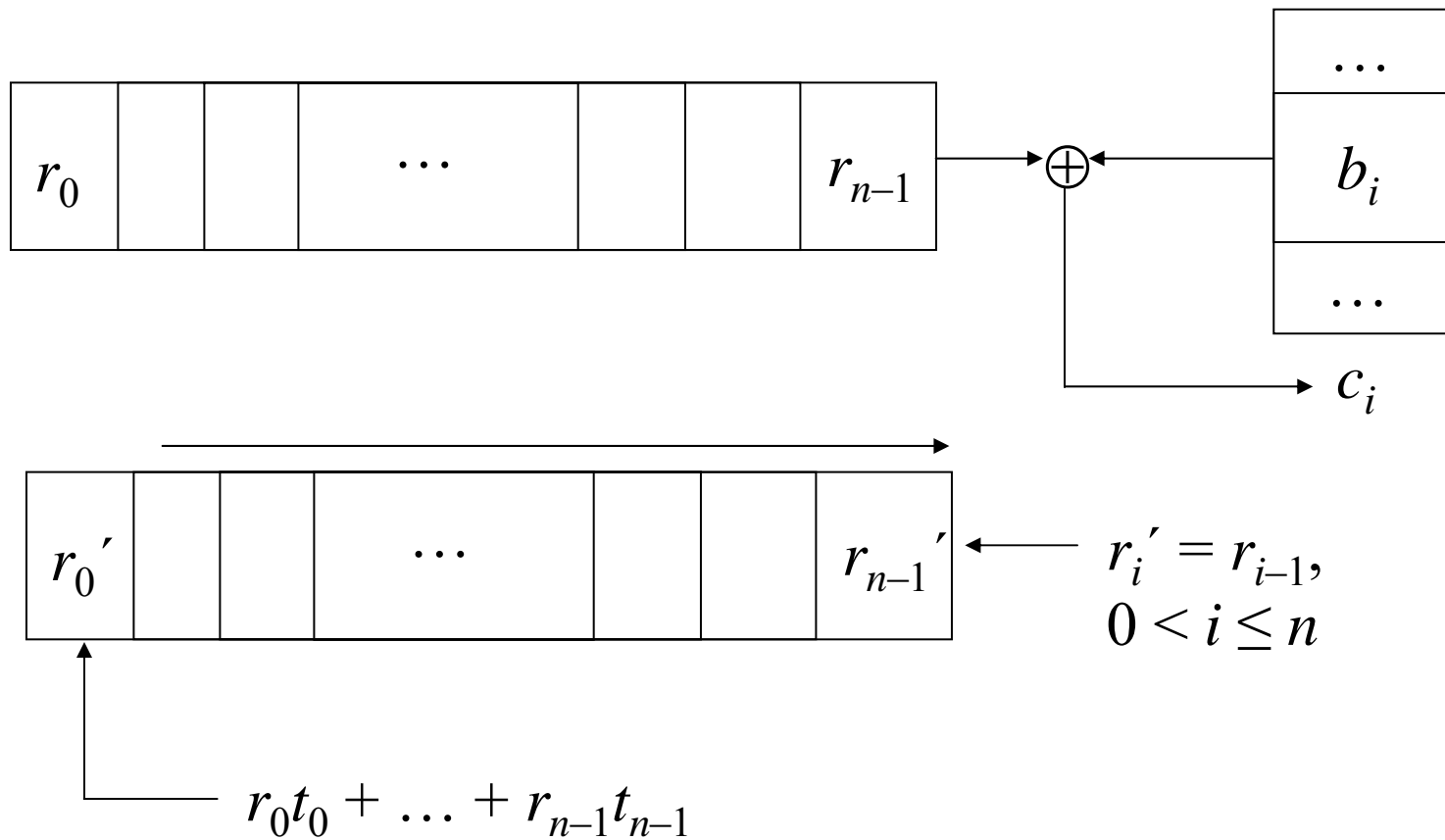
Chapter 10 CIPHER TECHNIQUES

- An *n*-stage Linear Feedback Shift Register:
 - *n* bit register $r = r_0 \dots r_{n-1}$
 - *n* bit tap sequence $t = t_0 \dots t_{n-1}$
 - To obtain a key bit:
 - Use r_{n-1}
 - Compute $x = r_0 t_0 \oplus \dots \oplus r_{n-1} t_{n-1}$
 - Shift r one bit to right, dropping r_{n-1}
 - Insert the new bit $x = r_0 t_0 \oplus \dots \oplus r_{n-1} t_{n-1}$
 - Example: Key sequence has period of 15 (010001111010110)

4-stage LFSR; $t = 1001$

	<u>r</u>	<u>k_j</u>	<u><i>new bit computation</i></u>	<u><i>new r</i></u>
Initial value →	0010	0	$01 \oplus 00 \oplus 10 \oplus 01 = 0$	0001
	0001	1	$01 \oplus 00 \oplus 00 \oplus 11 = 1$	1000
	1000	0	$11 \oplus 00 \oplus 00 \oplus 01 = 1$	1100
	1100	0	$11 \oplus 10 \oplus 00 \oplus 01 = 1$	1110
	1110	0	$11 \oplus 10 \oplus 10 \oplus 01 = 1$	1111
	1111	1	$11 \oplus 10 \oplus 10 \oplus 11 = 0$	0111
	1110	0	$11 \oplus 10 \oplus 10 \oplus 11 = 1$	1011

Chapter 10 CIPHER TECHNIQUES



Operation of Linear Feedback Shift Register

Chapter 10 CIPHER TECHNIQUES

- An n -stage Non-Linear Feedback Shift Register:
 - n bit register $r = r_0 \dots r_{n-1}$
 - To obtain a key bit:
 - Use r_{n-1}
 - Compute $x = f(r_0, \dots, r_{n-1})$; f is any function
 - Shift r one bit to right, dropping r_{n-1}
 - Insert the new bit $x = f(r_0, \dots, r_{n-1})$
 - Example: Key sequence has period of 4 (0011)

4-stage NLFSR; $f(r_0, r_1, r_2, r_3) = (r_0 \text{ and } r_2) \text{ or } r_3$

<u>r</u>	<u>k_i</u>	<u>new bit computation</u>	<u>new r</u>
1100	0	(1 and 0) or 0 = 0	0110
0110	0	(0 and 1) or 0 = 0	0011
0011	1	(0 and 1) or 1 = 1	1001
1001	1	(1 and 0) or 1 = 1	1100
1100	0	(1 and 0) or 0 = 0	0110
0110	0	(0 and 1) or 0 = 0	0011
0011	1	(0 and 1) or 1 = 1	1001

Chapter 10 CIPHER TECHNIQUES

- **NLFSRs are not common.**
 - There is no body of theory about how to build NLFSRs with long periods.
 - By contrast, it is known how to design n -stage LFSRs with a period of 2^n-1 . This period is maximal.
- **Self-Synchronous Stream Ciphers**
 - Self-synchronous stream ciphers obtain the key from the message itself.
 - The simplest self-synchronous stream cipher is called an autokey cipher.

Example: An autokey version of the Vigenere cipher

	unknown
	↓
key	XTHEBOYHASTHEBA
plaintext	THEBOYHASTHEBAG
ciphertext	QALFPNFHSLALFCT

Note that this type of cipher is weak.

The last two letters of the plaintext “THE” produces the ciphertext “AL” because H is enciphered with the key letter T, and E is enciphered with the key letter H.

Chapter 10 CIPHER TECHNIQUES

- An alternative is to use the ciphertext as the key stream.

Example: An autokey version of the Vigenere cipher

	unknown
	↓
key	XQXBCQOVVNGNRTT
plaintext	THEBOYHASTHEBAG
ciphertext	QXBCQOVVNGNRTTM

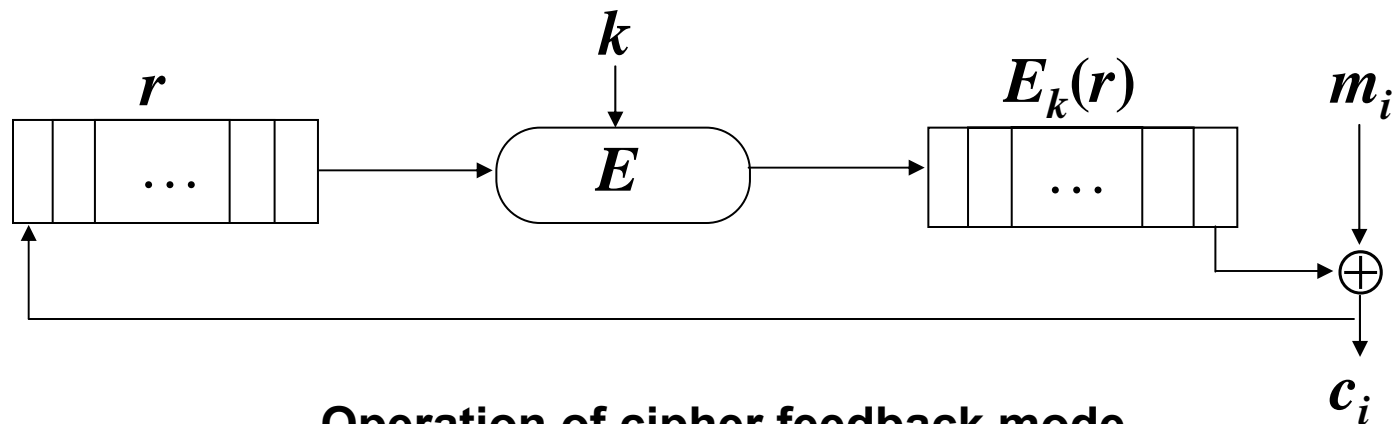
If the key is derived from the ciphertext, it eliminates the repetition "ALF."

Note that this type of cipher is also weak.

The letter X in the ciphertext is the result of enciphering a plaintext letter with the key Q. The unknown plaintext letter is H!

The cryptanalyst can reconstruct all of the plaintext except for the first character.

Chapter 10 CIPHER TECHNIQUES



Operation of cipher feedback mode

- A variant of the autokey cipher is the cipher feedback mode.
 - If a bit is corrupted in transmission of the ciphertext, the next n bits will be deciphered incorrectly.
 - After receiving n uncorrupted bits, the shift register will be reinitialized to the value used for encipherment and the ciphertext will decipher properly from that point on.
- E is an encipherment function.
 - k is a cryptographic key.
 - r is a register.
 - To obtain a bit for the key, compute $E_k(r)$.
 - The rightmost bit of the output is xored with one bit of the message.
 - The resulting ciphertext is fed back into the left most bit of the register r .

Chapter 10 CIPHER TECHNIQUES

- **Block Ciphers**

- Encipher and decipher multiple bits at once.
- Software implementations of block ciphers are faster than those of stream ciphers.
- Errors in transmitting one block do not affect other blocks.
- If each block is enciphered independently, using the same key, identical plaintext blocks will result in identical ciphertext blocks.
- This allows the cryptanalyst to determine the ciphertext of a specific plaintext block.
- **EXAMPLE:** A banking database with 2 records.

Member:	HOLLY	INCOME	\$100,000
Member:	HEIDI	INCOME	\$100,000

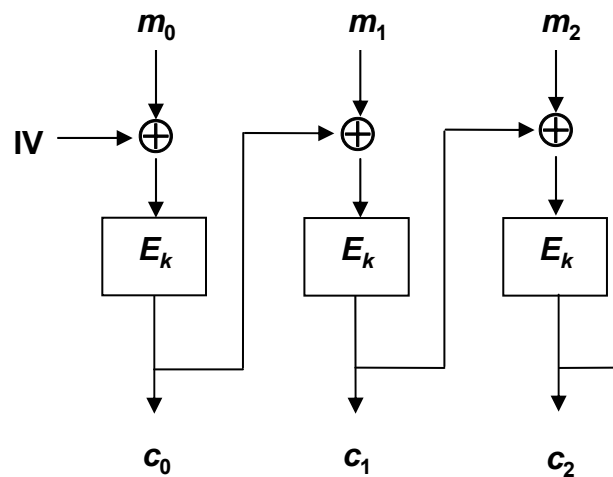
The corresponding ciphertext is:

ABCQZRME	GHQMRSIB	CTXUVYSS	RMGRPFQN
ABCQZRME	ORMPABRZ	CTXUVYSS	RMGRPFQN

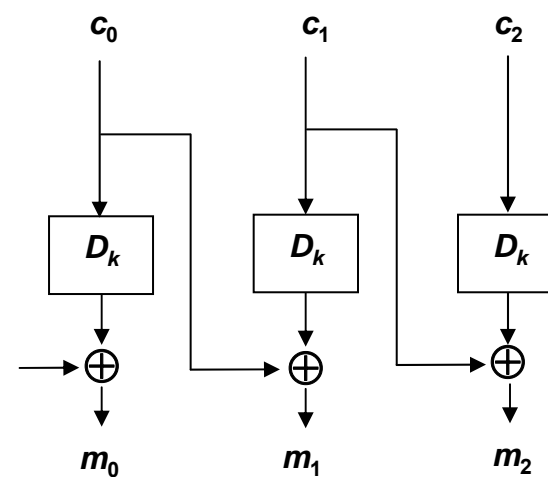
If an attacker is able to determine who these records belong to, and that ciphertext “CTXUVYSS” corresponds to “INCOME,” he will know that both Holly and Heidi have the same income!

Chapter 10 CIPHER TECHNIQUES

- To prevent this type of attack, cipher block chaining is a solution.
- Cipher Block Chaining (CBC)
 - Exclusive-or current plaintext block with previous ciphertext block:
 - $c_0 = E_k(m_0 \oplus I)$, where I is the initialization vector.
 - $c_i = E_k(m_i \oplus c_{i-1})$ for $i > 0$



CBC encryption



CBC decryption

Chapter 10 CIPHER TECHNIQUES

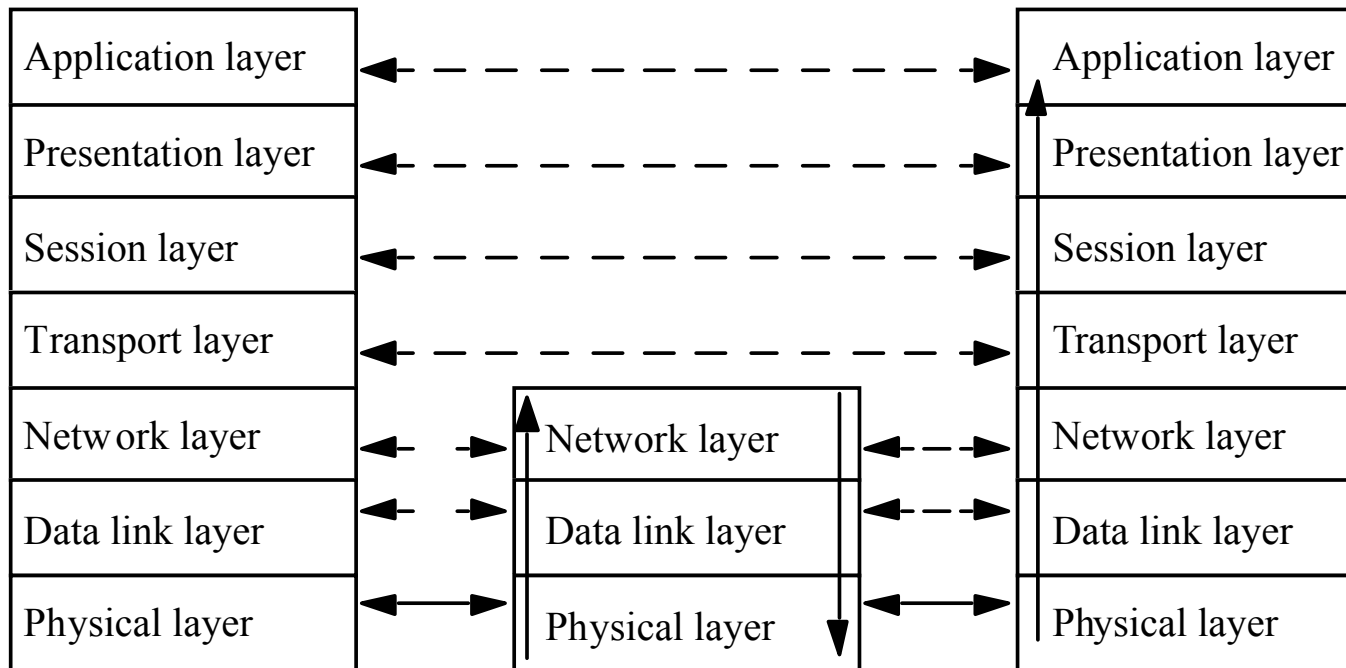
- **Multiple Encipherment**
 - **Double encipherment:**
 - k and k' are two keys, each key of length n
 - $c = E_{k'}(E_k(m))$
 - Effective key length is $2n$
 - **Encrypt-Decrypt-Encrypt (EDE) mode**
 - $c = E_k(D_{k'}(E_k(m)))$
 - The DES in EDE mode is widely used in the financial world.
 - The DES in EDE is a standard (ANSI X9.17 and ISO 8732).
 - **Encrypt-Encrypt-Encrypt (EEE) mode**
 - k , k' , and k'' are three keys
 - $c = E_k(E_{k'}(E_{k''}(m)))$

Chapter 10 CIPHER TECHNIQUES

10.3 Networks and Cryptography

- The International Standard Organization/Open System Interconnect (ISO/OSI) network model is composed of seven layers.
 - Each host has a principal at each layer that communicates with a peer on other hosts.
 - Layer 1,2,3 principals interact only with similar principles at neighboring hosts.
 - Principals at layers 4,5,6, and 7 interact only with similar principals at the other end of the communication.
- Hosts C_0, \dots, C_n be such that C_i and C_{i+1} are directly connected, for $0 \leq i < n$.
 - A communications protocol that has C_0 and C_n as its end points is called an end-to-end protocol.
 - A communications protocol that has C_i and C_{i+1} as its end points is called a link protocol.

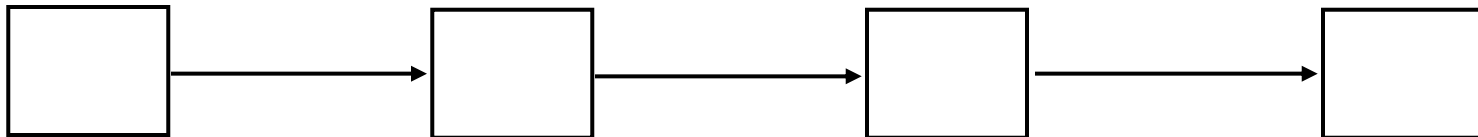
Chapter 10 CIPHER TECHNIQUES



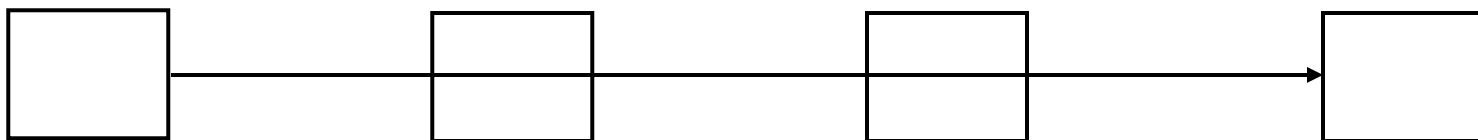
ISO/OSI model

Chapter 10 CIPHER TECHNIQUES

Link Protocol



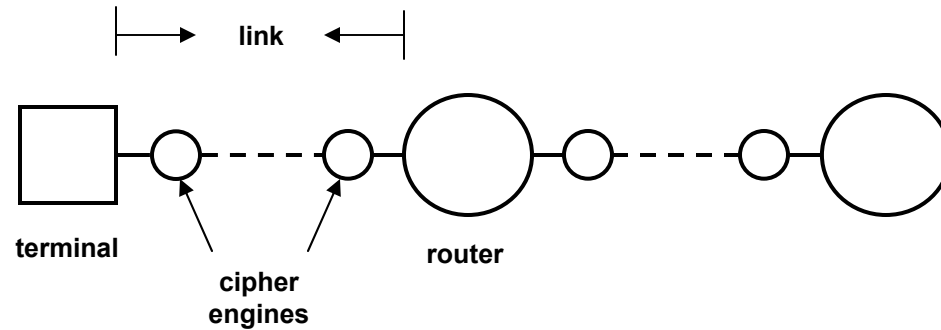
End-to-End Protocol



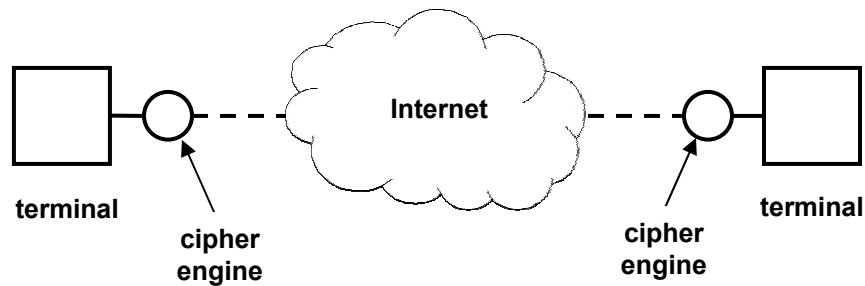
Chapter 10 CIPHER TECHNIQUES

- The difference between an end-to-end protocol and a link protocol:
 - In an end-to-end protocol, the intermediate hosts play no part.
 - In a link protocol, the role of each pair of intermediate hosts is described to process each message.
- Each type of protocol involves cryptology.
- When encryption is used in an end-to-end protocol, we use the term end-to-end encryption.
- When encryption is used in a link protocol, we use the term link encryption.
- In end-to-end encryption, each host shares a cryptographic key with each destination.
- In link encryption, each host shares a cryptographic key with its neighbor.

Chapter 10 CIPHER TECHNIQUES



Link Encryption



End-to-End Encryption

Chapter 10 CIPHER TECHNIQUES

10.4 Example Protocols

- **Application Layer**: Privacy-Enhanced Mail (PEM) is an Internet standard that provides for secure exchange of electronic mail.
- **Transport Layer**:
 - **Secure Sockets Layer (SSL)** is developed by Netscape for transmitting private documents via the Internet.
 - SSL runs on layers beneath application protocols such as HTTP, and above the TCP transport protocol.
 - **Transport Layer Security (TLS)** is successor to SSL.
- **Network Layer**: IP Security (IPsec) is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer.