Cipher Techniques on Networks

Amit Konar

Math and CS, UMSL

Why to learn Cipher Techniques on Networks?

Because

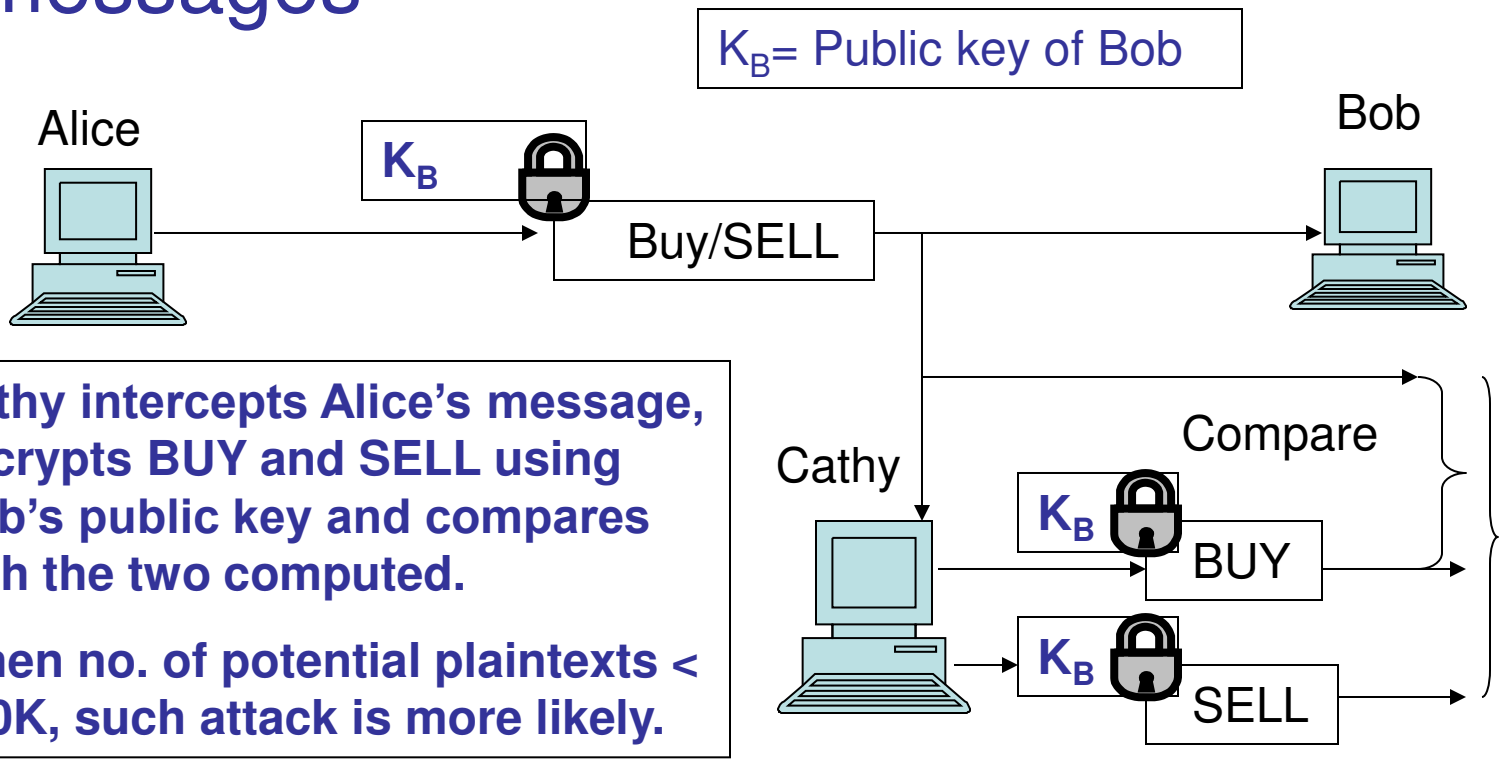
1) Cryptographic systems are sensitive to environments,

2) using cryptography on networks thus introduces many problems,

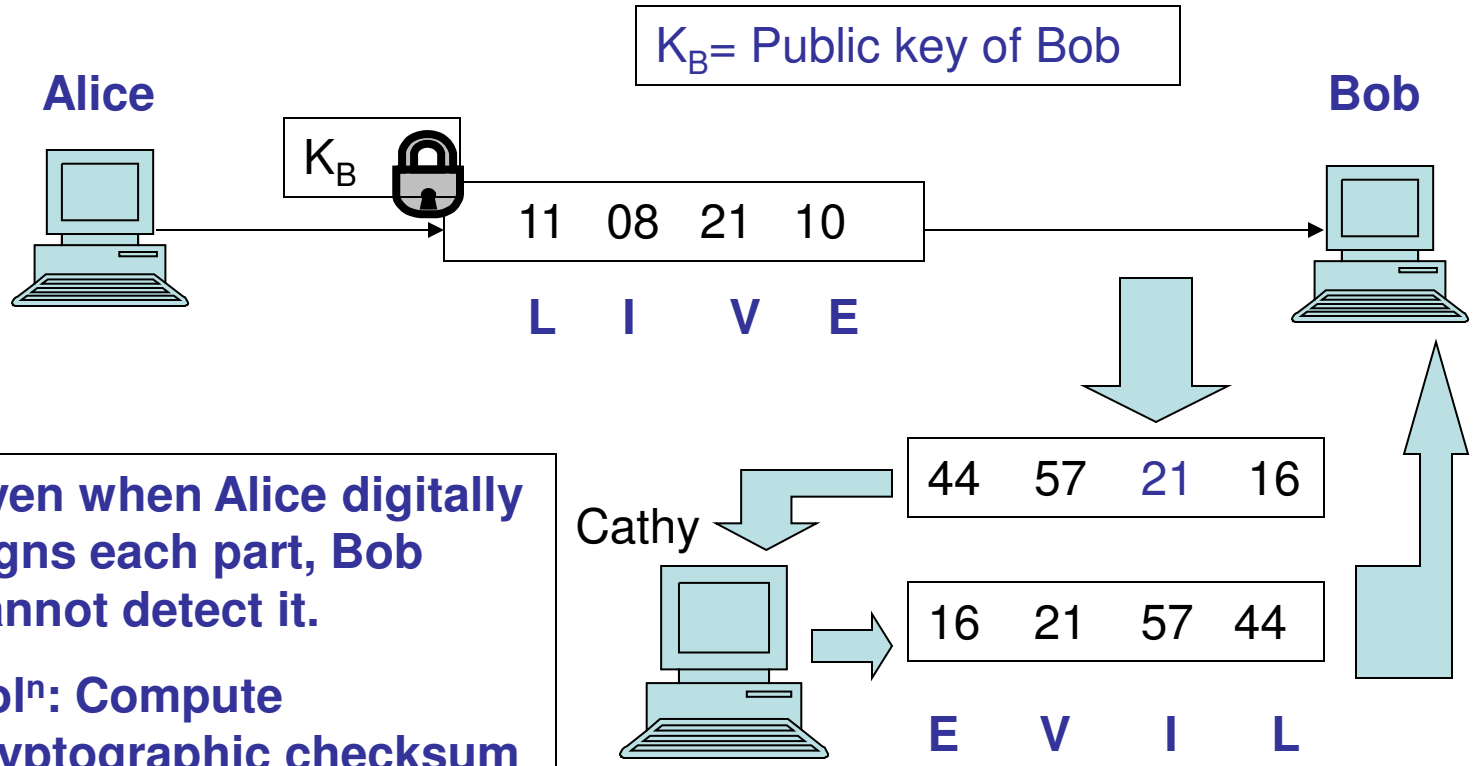
Observation: Stream and Block ciphers have been found to be most convenient for realization of cryptography on computer networks.

Sensitivity of Cryptographic Systems to Environment

Example 1: Pre-computing the possible messages



Example 2: Sensitivity to Environment: Misordered Blocks



Even when Alice digitally signs each part, Bob cannot detect it.

Sol^n: Compute cryptographic checksum and sign that value.

Example 3: Sensitivity to Environment:Statistical Regularities

Plaintext: HELLO WORLD

Ciphertext: KHOOR ZRUOG

Technique: Caeser Cipher

When the same word “world” appears once again, ciphertext will be same. Such structure of information in ciphertexts is helpful for the intruders to determine plaintext.

Definition: Block Cipher

Let

message $m = b_1\ b_2\ \ldots.$,

where b_i has a fixed length.

Then a **block cipher** is a cipher for which the encipherment algorithm

$E_k(m) = E_k(b_1)\ E_k(b_2)\ldots..$

where k is a given key.

Example: DES. It breaks the message into 64-bit blocks, and uses the same 56-bit key to encipher each block.

Definition: Stream Cipher

Let

message m= b_1 b_2 …,

where each b_i has a fixed length.

Let k= k_1 k_2…. be the keys for each stream of binary data b_1, b_2…

Then a **stream cipher** is a cipher for which

$E_k(m)= E_{k1}(b_1)\ E_{k2}(b_2)$…

Example: Vigenere Cipher, where b_i is the character of the message, and k_i is a character of the key.

Synchronous Stream Ciphers

Let

$r = r_0\ r_1\ \ldots r_{n-1}$ be a n-bit linear feedback register, and

$t = t_1\ t_2 \ldots\ldots t_{n-1}$ be a n-bit tap sequence.

r_{n-1} is used as key.

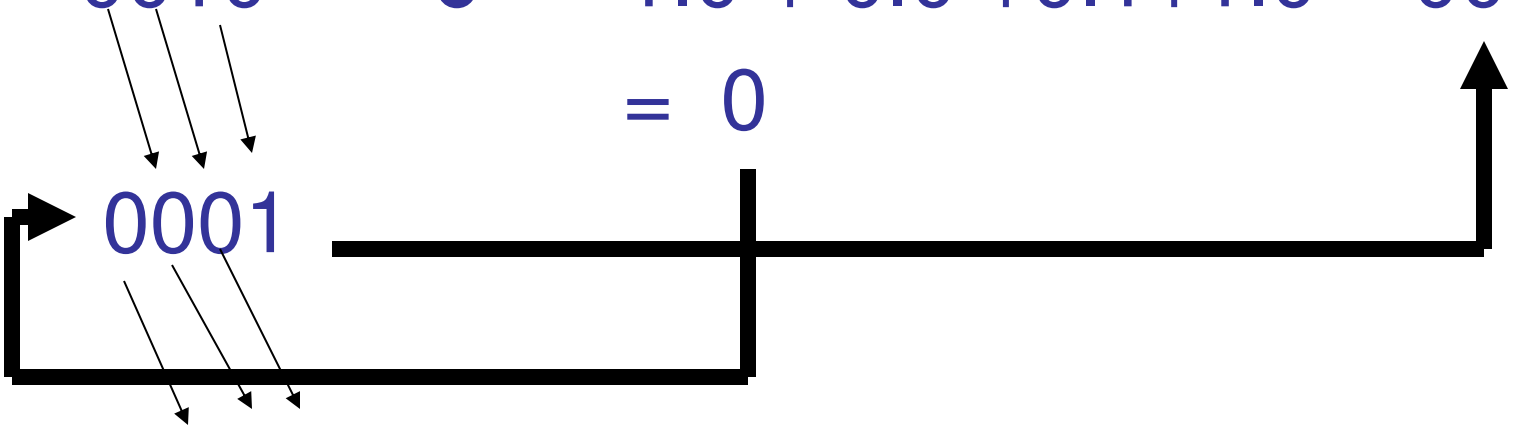
Evaluate r_0t_0 xor r_1t_1 xor …xor $r_{n-1}t_{n-1}$,

Shift the register r right by one bit and insert the evaluated result as r_0. The register r is called **n-stage linear feedback register**.

Example: Synchronous Stream Ciphers

Let **tap sequence**= 1001.

Current Reg.	**Key**	**New bit**	**New Reg.**
0010	**0**	1.0 + 0.0 +0.1+1.0 = 0	0001



Key stream thus generated: 010001111010110

Limitations of Linear Feedback Shift Register based Stream Cipher

1. If the key is shorter than the message, breaking part of the ciphertext gives cryptoanalysts information about other parts of the ciphertext.
2. For an LFSR, a known plaintext attack can reveal parts of the key sequence.
3. If the known plaintext is of length 2n, the tap sequence for an n-stage LFSR can be determined completely.

Synchronous Stream Ciphers with Nonlinear Feedback Shift Register

Let

$r = r_0\, r_1 \ldots r_{n-1}$ be a n-bit register,

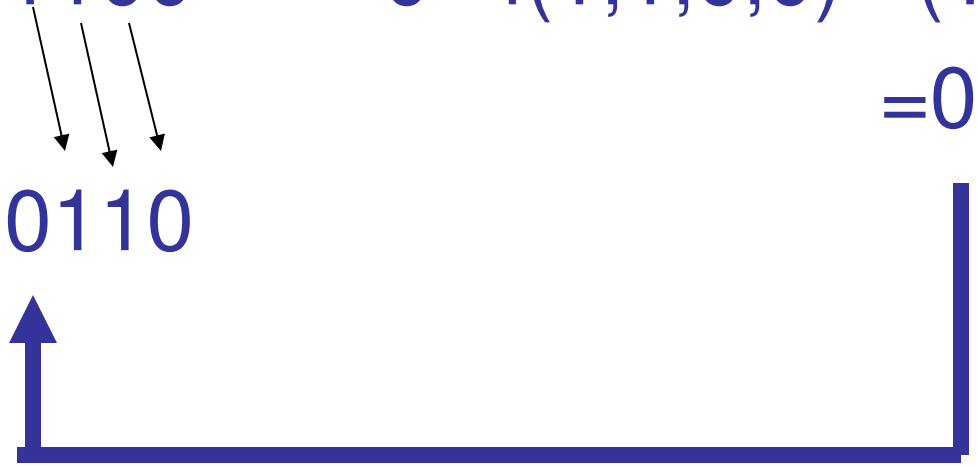
$f(r_0, r_1, \ldots, r_{n-1})$ be a nonlinear function.

Then if we shift the register right by one bit and f() is inserted in the r_0 bit-position, we call the system a **Non-linear Feedback Shift Register.**

Example: Non-linear Feedback shift Register

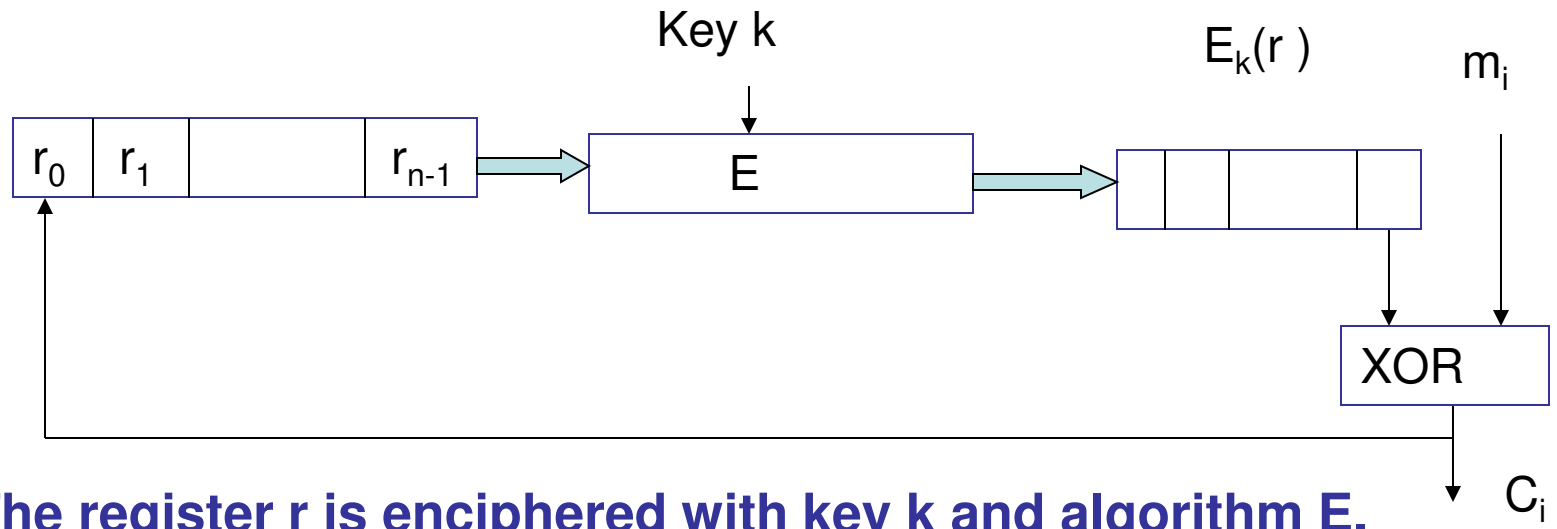
Let

Current Reg.	**Key**	**New Bit**	**New Reg.**
		$(r_0$ and $r_2)$ or r_3	
1100	0	f(1,1,0,0) =(1 and 0)or 0	0110
		=0	
0110			



Merits: No tap sequence needed.

Block Ciphers



The register r is enciphered with key k and algorithm E. The register r is shifted right and the m_i xor $E_k(r_{n-1}) = C_i$ is placed at r_0 position.

Scope of attack: Since each block is enciphered independently using the same key, identical plaintext blocks produce identical ciphertexts.

Example: Scope of Attack in Block Ciphers

Plaintext:

MEMBER HOLY INCOME $100K

MEMBER HEIDI INCOME $100k

Ciphertext:

ABCQZRME GHQMRSIB CTXUVYSS RMGRPFQN

ABCQZRME ORMPABRZ CTXUVYSS RMGRPFQN

If the attackers knows CTXUVYSS is the encipherment of INCOME, and he knows HOLY and HEIDI, then he can easily identify that the income of both people are same.

How to overcome this problem?

To prevent this, **some information related to blocks' position is inserted into the plaintext blocks before it is enciphered**. The information could be sequence no. of repeated blocks.

The disadvantage is that effective block size is reduced because fewer message bits are present in a block.

Cipher Block Chaining

Advantage: It does not require extra information to occupy bit spaces; so every bit in the block is part of the message.

Let

E_k be the encipherment algo. with key k,

I- initialization vector, m = message

Then cipher block chaining technique is

$C_0 = E_k(m_0 \text{ xor } I)$,

$C_i = E_k(m_i \text{ xor } C_{i-1})$ for $I > 0$

Multiple Encryption

Let

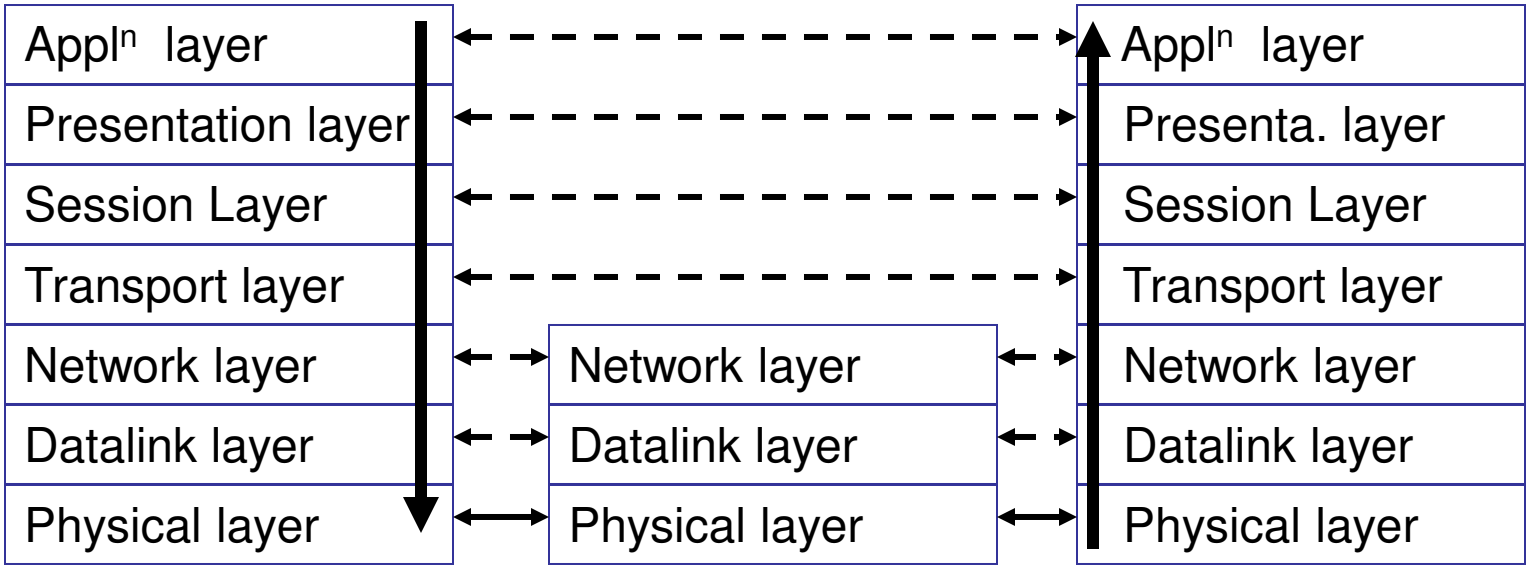
two keys be k' and k.

Encipherment algo. Is

$C = E_{k'}(E_k(m))$

Merits: It has an effective key length of 2n whereas keys to E are of length n.

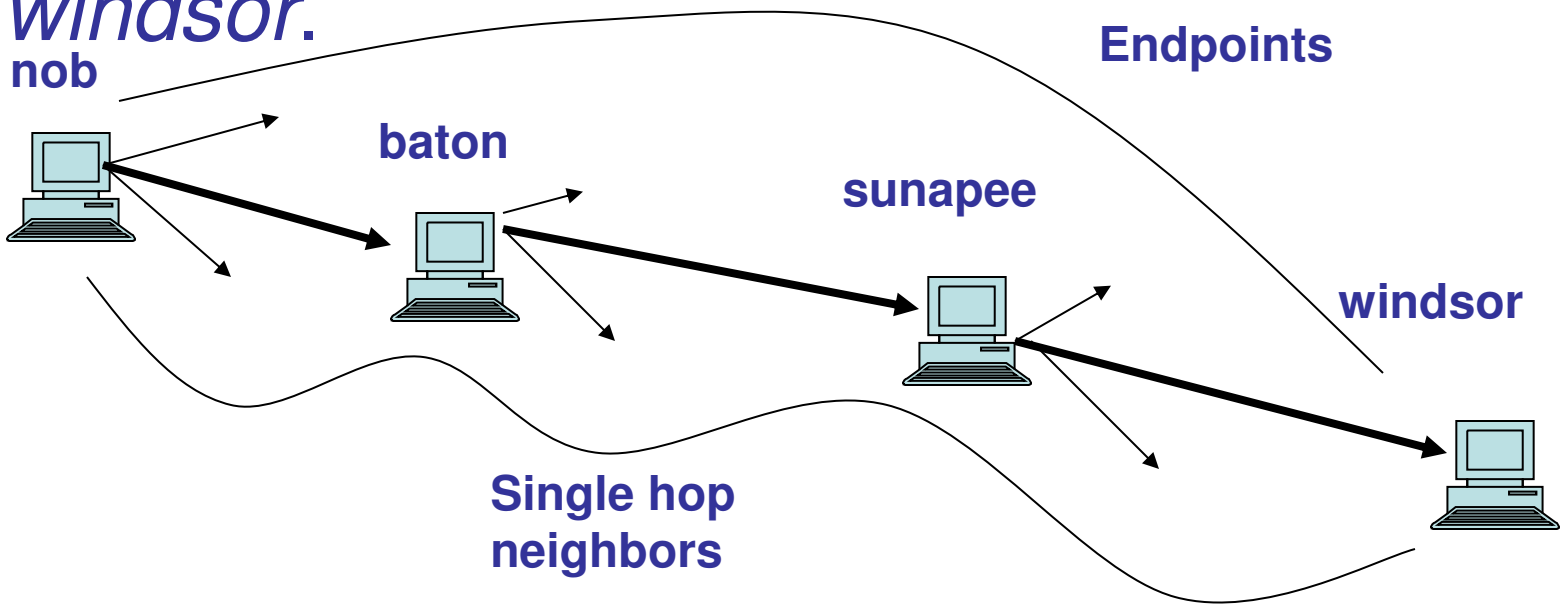
Communication Protocol in Computer Networks



The ISO/OSI model: The dashed arrow indicates peer-to-peer communication. For example, transport layers are communicating with each other. The solid arrows indicate actual flow of bits. For example, the transport layer invokes network layer routines on local host, which invokes data link layer routines, which puts the bits onto the network. The physical layer passes the bits to the next hop, or host on the path.

Example: How communication takes place from one host to another?

Host *nob* wants to send a message to host *windsor*.



Solid lines indicate message flow path to the nearest host through a routing protocol.

End-to-End and Link Protocol

Let hosts C_0, C_1,…, C_n be such that C_i and C_{i+1} are directly connected, for $0<=i<=n$.

A communication protocol that has $C_0$and C_n as its end points is called **end-to-end protocol.**

A communication protocol that has C_j and C_{j+1} as its endpoints is called a **link protocol.**

Difference between End-to-end and Link Protocols

The **intermediate hosts play no roles in an end-to-end protocol** other than forwarding the messages.

On the other hand, **a link protocol describes how each pair of intermediate hosts process each message**.

Cryptographic Protocols: Link Encryption and End-to-End Encryption

- In Link Encryption, the encryption and decryption takes place between two neighboring hosts.

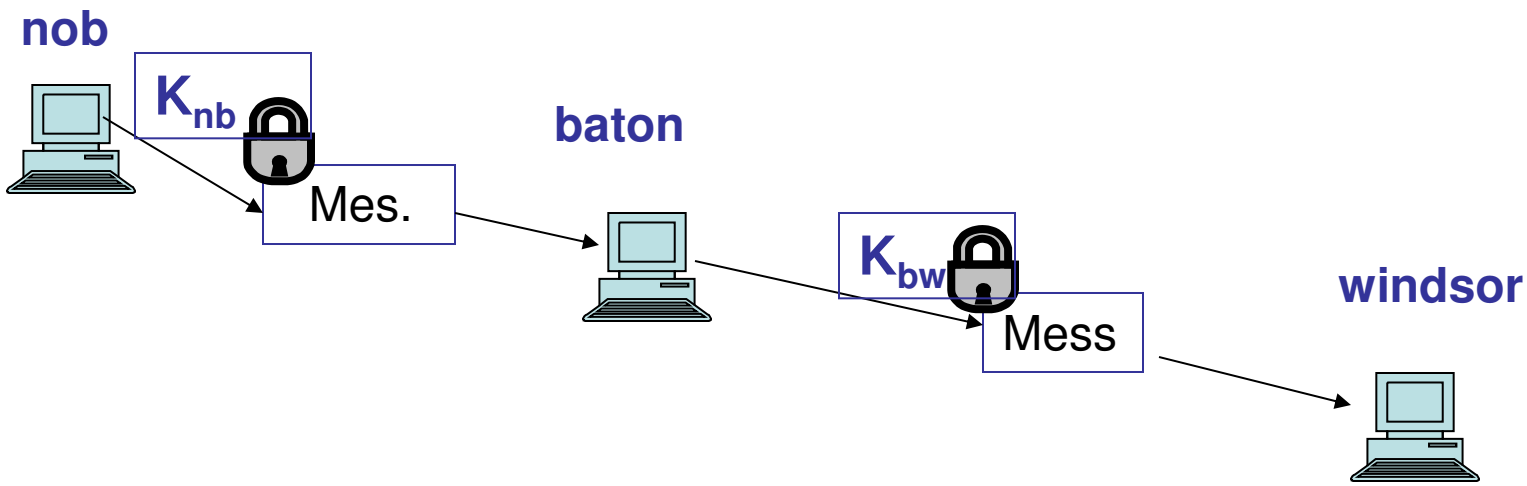
- In End-to-End encryption, the encryption and decryption takes place between end-to-end hosts.

Link Encryption

In link encryption,

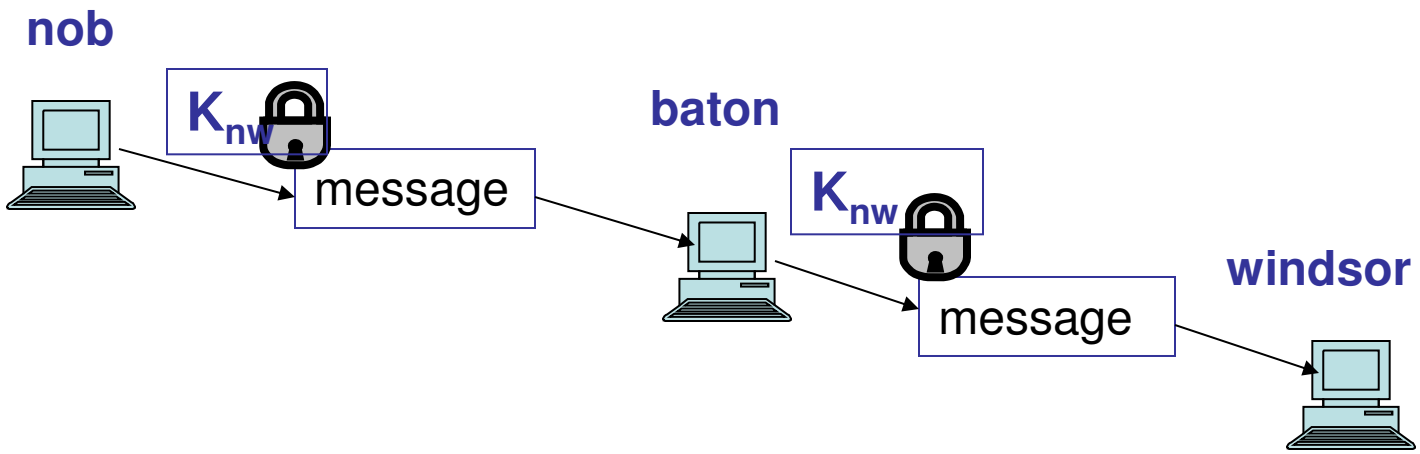
1. Each host shares a cryptographic key with its neighbor.
2. Keys may be distributed on per host-pair basis/ individual private plus public key basis.
3. Message is encrypted by the sender, and decrypted at the neighborhood link host.
4. For each next hop, the messages are re-enciphered with a different key.

Example: Host *nob* likes to send message to host *windsor* using link encryption



Nob encrypts the message using K_{nb}, shared key between nob and baton; baton decrypts it and re-encrypts with K_{bw}, the shared key between baton and windsor; windsor decrypts it and gets the message.

Example: Host nob wants to send a message to a distant host windsor using End-to-End encryption



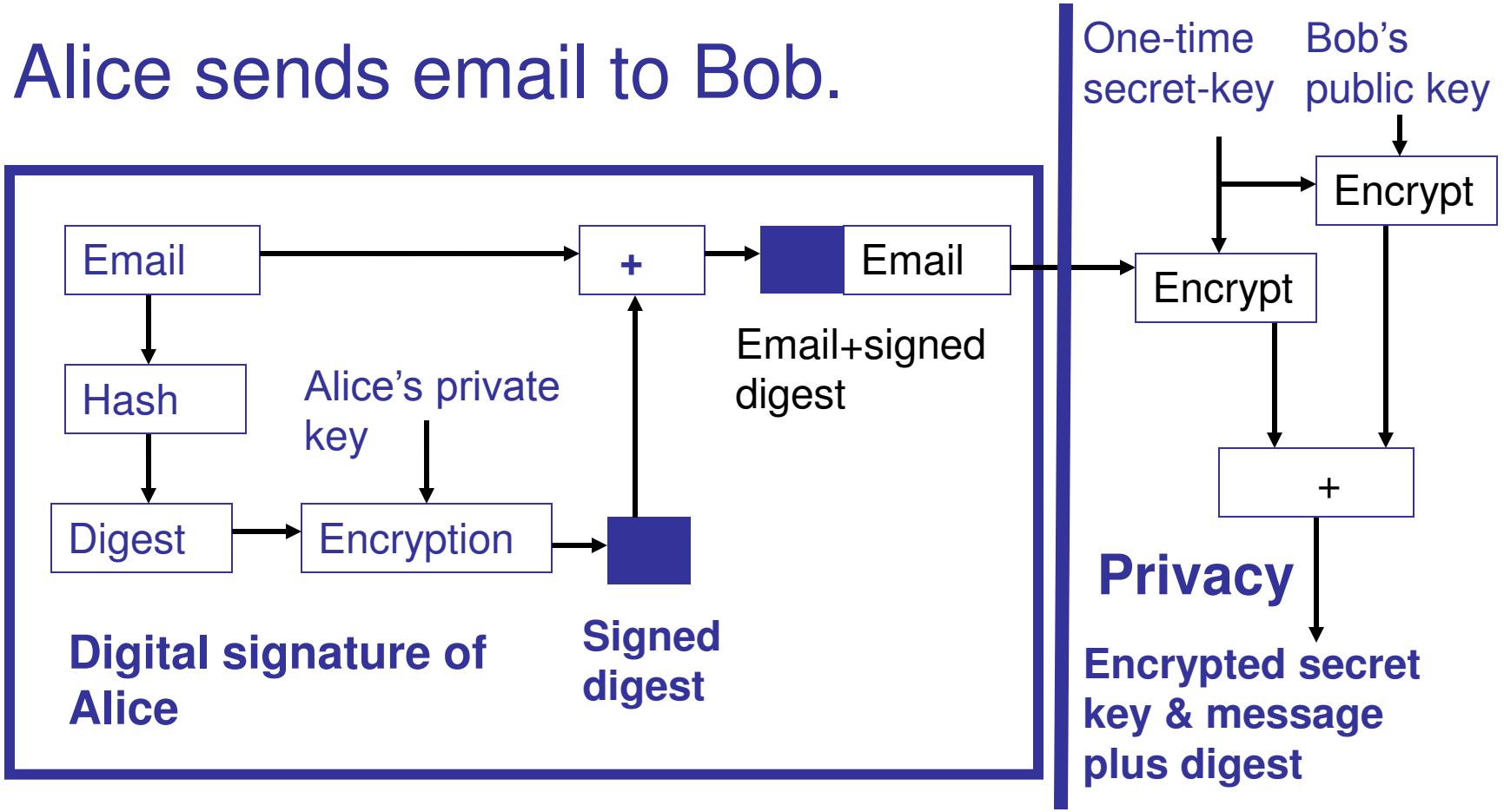
nob encrypts the message with K_{nw} and baton simply forwards it to windsor. Windsor decrypts it and gets the message.

Security Protocols at Different Layer

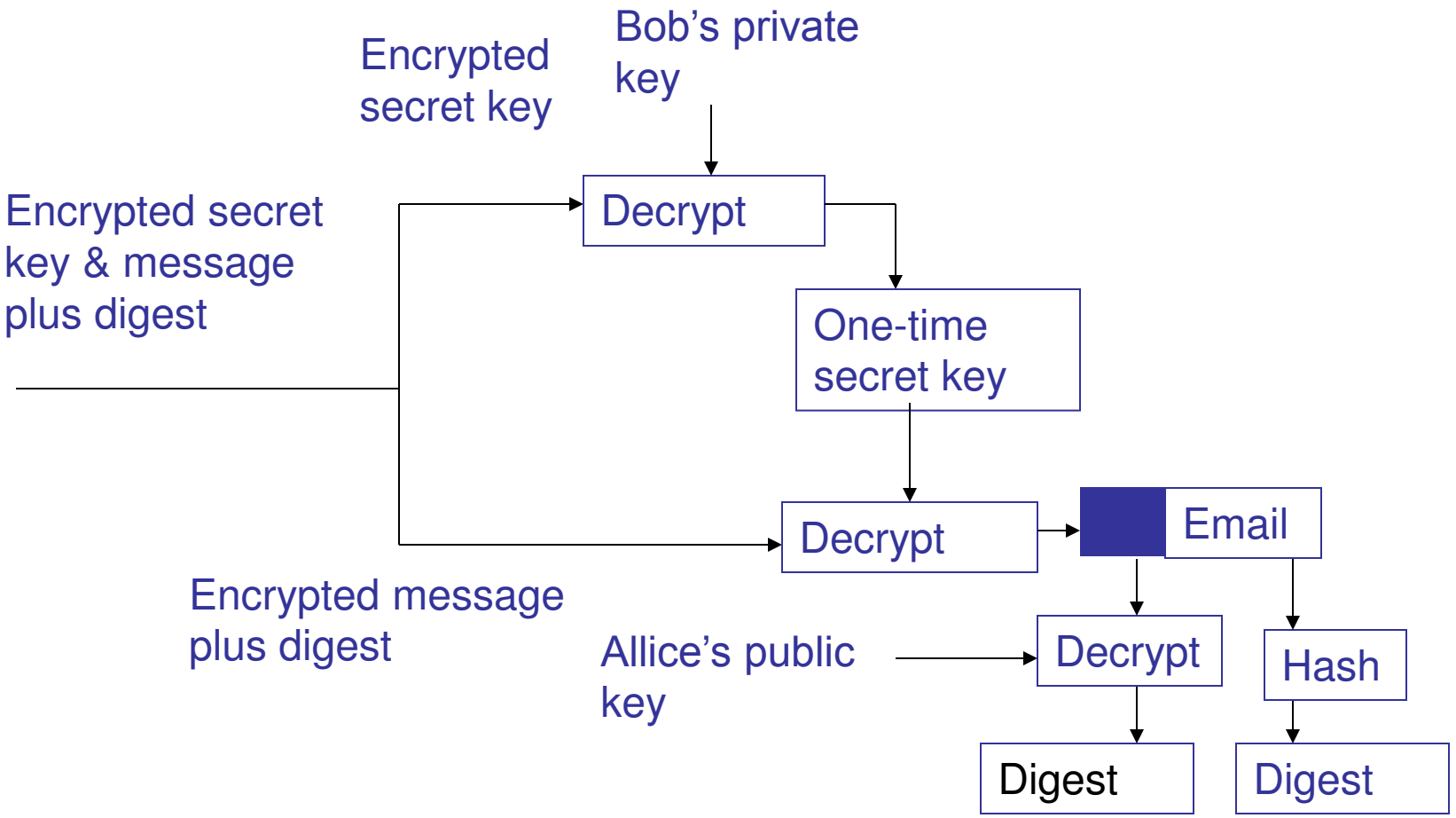
LAYER	PROTOCOL
Application layer	Pretty Good Privacy (PGP)
Transportation Layer	Security Socket layer (SSL)
IP layer	IP Security (IPSec)

Pretty Good Service (PGP)
Protocol: Secure Email service

Alice sends email to Bob.



Decryption at Bob's site



Transportation Layer Security: Why needed?

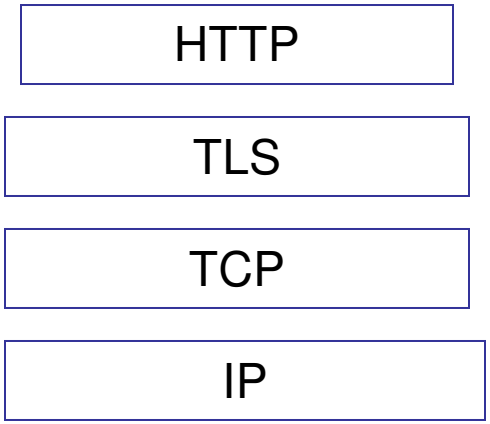
For transactions on the internet, a browser needs the following:

1. The customer needs to be sure that the server belongs to the actual vendor, not an imposter. For example, a customer does not want to give an imposter her credit card no. In other words, the server must be authenticated.

Why Transportation layer security?

2. The customer must be sure that the contents of the message are not modified during transaction. A bill of $100 should not be changed to $1000. The integrity of the message must be preserved,
3. The customer needs to know that the imposter does not intercept sensitive information, such as credit card no. There is a need for privacy.

Position of Transport Layer security



The application layer protocol HTTP uses the services of TLS, and TLS in turn uses the services of transportation layer.

Handshake Protocol in Transport Layer Security