Confidentiality Using Symmetric Encryption

Tsay, Yih-Kuen

Dept. of Information Management

National Taiwan University

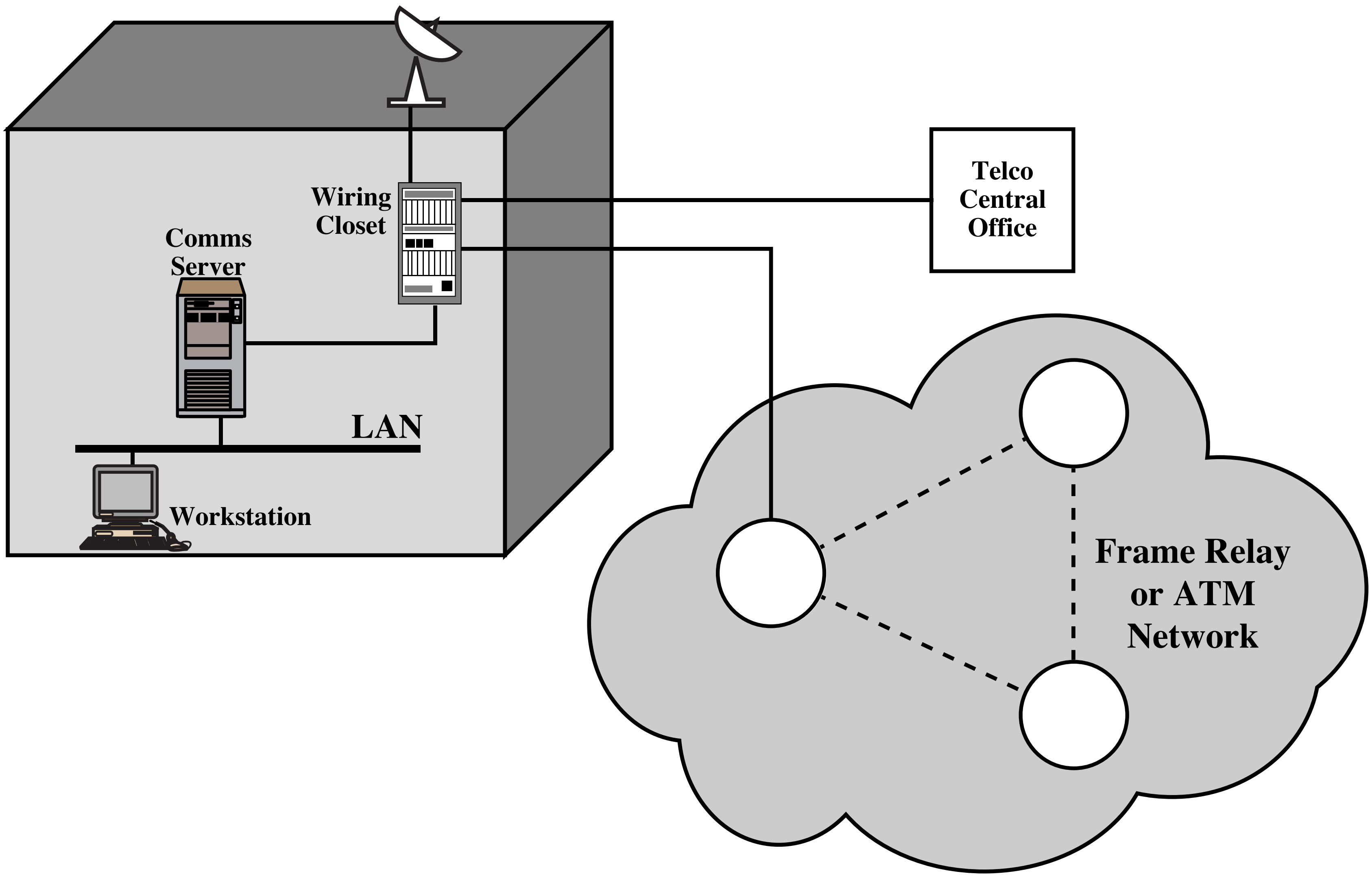
Confidentiality

- Providing confidentiality through the use of secret-key encryption has historically been the focus of cryptology.
- This topic remains important in itself, though other considerations have emerged in the last few decades.
- An understanding of the issues involved here
  - clarifies those in other applications of encryption and
  - helps to motivate the development of public-key encryption.

Placement of Encryption Function

- Issues involved:
  - What should be encrypted?
  - Where should encryption be done?
- Two approaches:
  - Link encryption
  - End-to-end encryption
- To make the decisions, one should first examine the potential locations of security attacks.

Points of Vulnerability



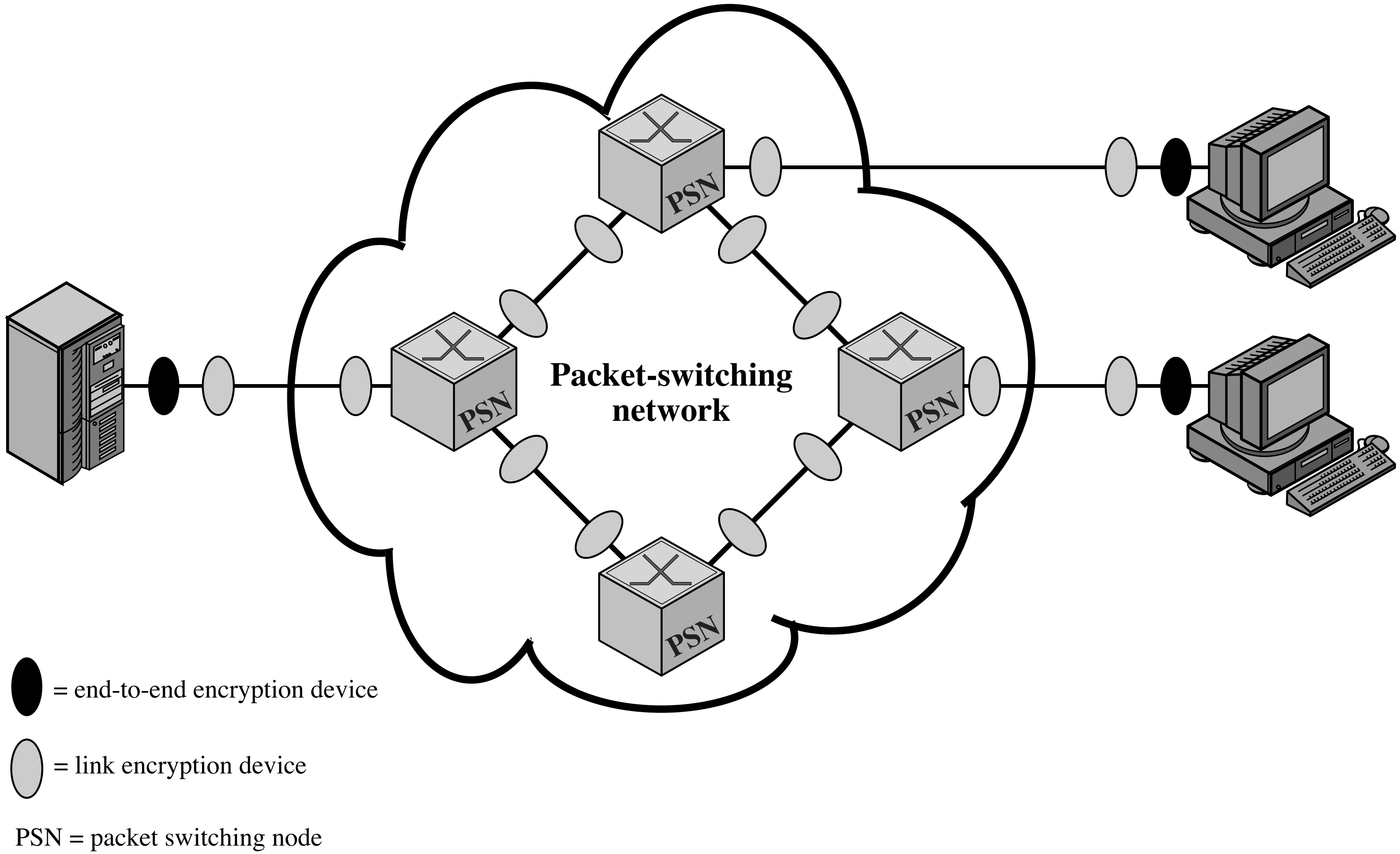
Source: Figure 7.1, Stallings 2006

Locations for Confidentiality Attacks

Consider a user workstation in a typical business organization. The points of vulnerability include:

- The LAN that the workstation is attached to: *eavesdropping* on the LAN, which is typically a *broadcast* network.
- The Wiring closet: tapping the wires.
- Communications links out of the Wiring closet: invasive or inductive tapping.
- Processors along the path to the outside: modifying the hardware or software, etc.

Encryption in Packet-Switching Networks



Source: Figure 7.2, Stallings 2006

Link Encryption

- Each vulnerable communications link is equipped on both ends with an encryption device. Thus, all traffic over all communications links is secured.
- The message must be decrypted each time it enters a packet switch. Thus, the message is vulnerable at each switch.
- Many keys must be provided. However, each key needs be distributed to only two nodes.

End-to-End Encryption

- The encryption process is carried out at the two end systems. The source and the destination share a key.
- This plan seems to secure the transmission against attacks on the network links or switches. There is, however, still a weak spot.
- The source may encrypt only the user data portion, but must leave the header in the clear.
- With end-to-end encryption, the user data are secure, but the traffic pattern is not. A certain degree of authentication is also provided.

Link vs. End-to-End Encryptions

Link Encryption	End-to-End Encryption
Security within End Systems and Intermediate Systems	
Message exposed in sending host Message exposed in intermediate nodes	Message encrypted in sending host Message encrypted in intermediate nodes
Role of User	
Applied by sending host Transparent to user Host maintains encryption facility One facility for all users Can be done in hardware All or no messages encrypted	Applied by sending process User applies encryption User must determine algorithm Users selects encryption scheme Software implementation User chooses to encrypt, or not, for each message
Implementation Concerns	
Requires one key per (host-intermediate node) pair and (intermediate node-intermediate node) pair Provides host authentication	Requires one key per user pair Provides user authentication

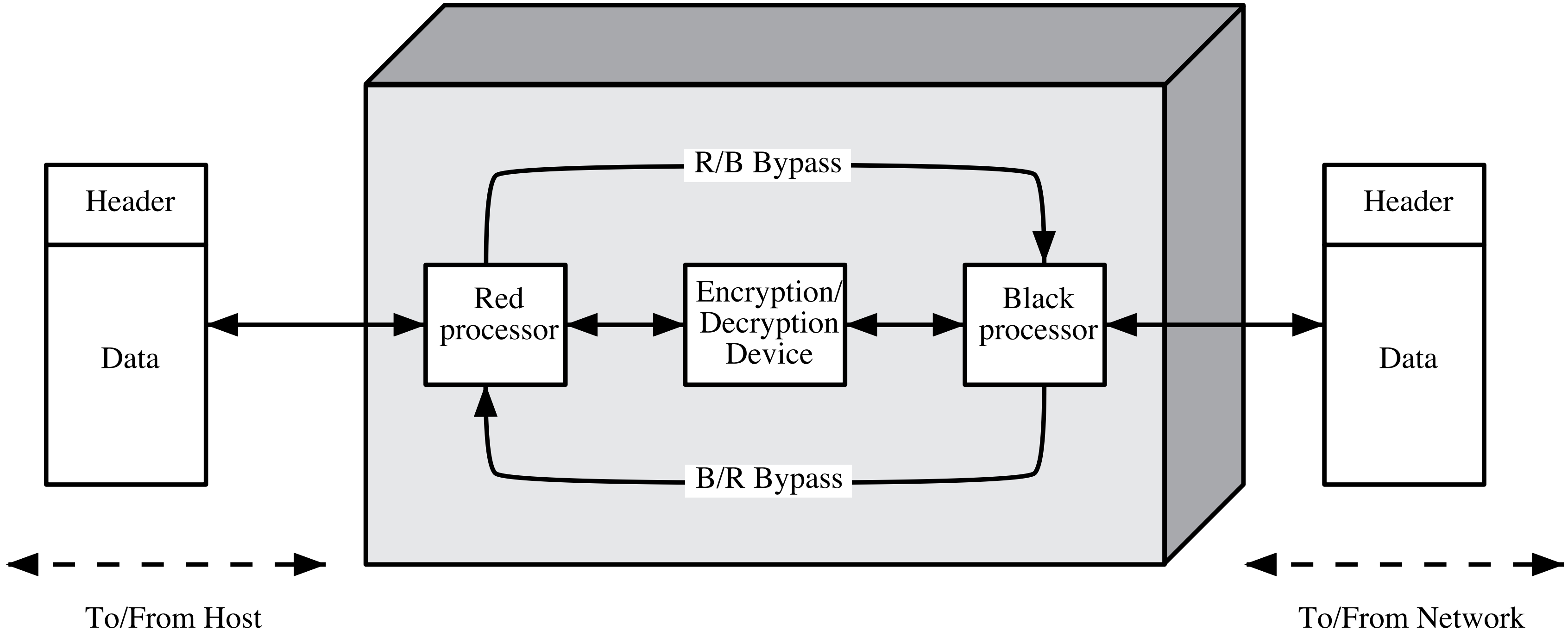
Source: Table 7.1, Stallings 2006

Deploying End-to-End Encryption

Possible choices:

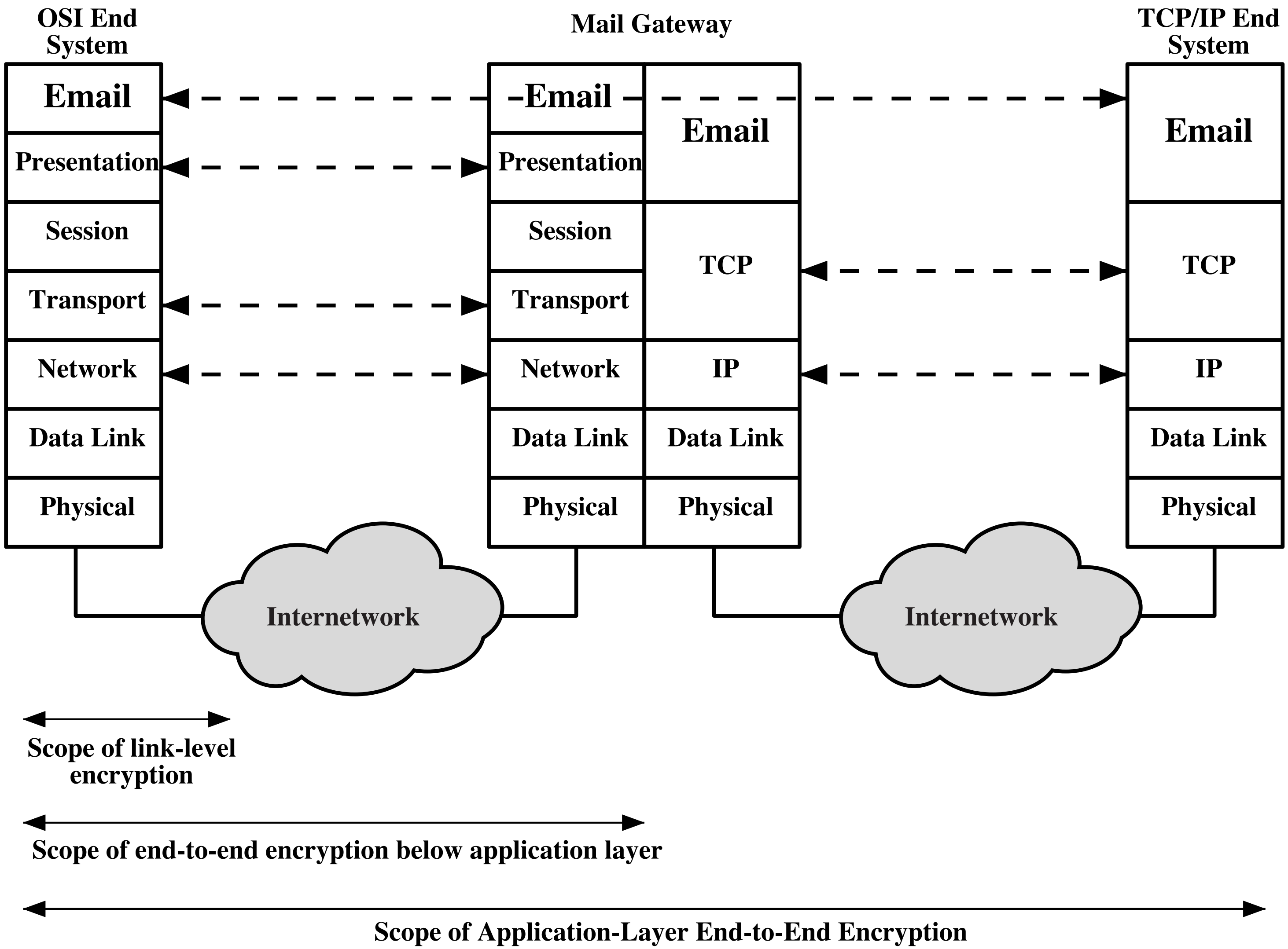
- The network layer or the transport layer
  - one key for each pair of end systems
  - cannot cross internetwork boundaries
- The application layer
  - many keys needed: one key for each pair of users
  - can cross internetwork boundaries

Front-End Processor Function



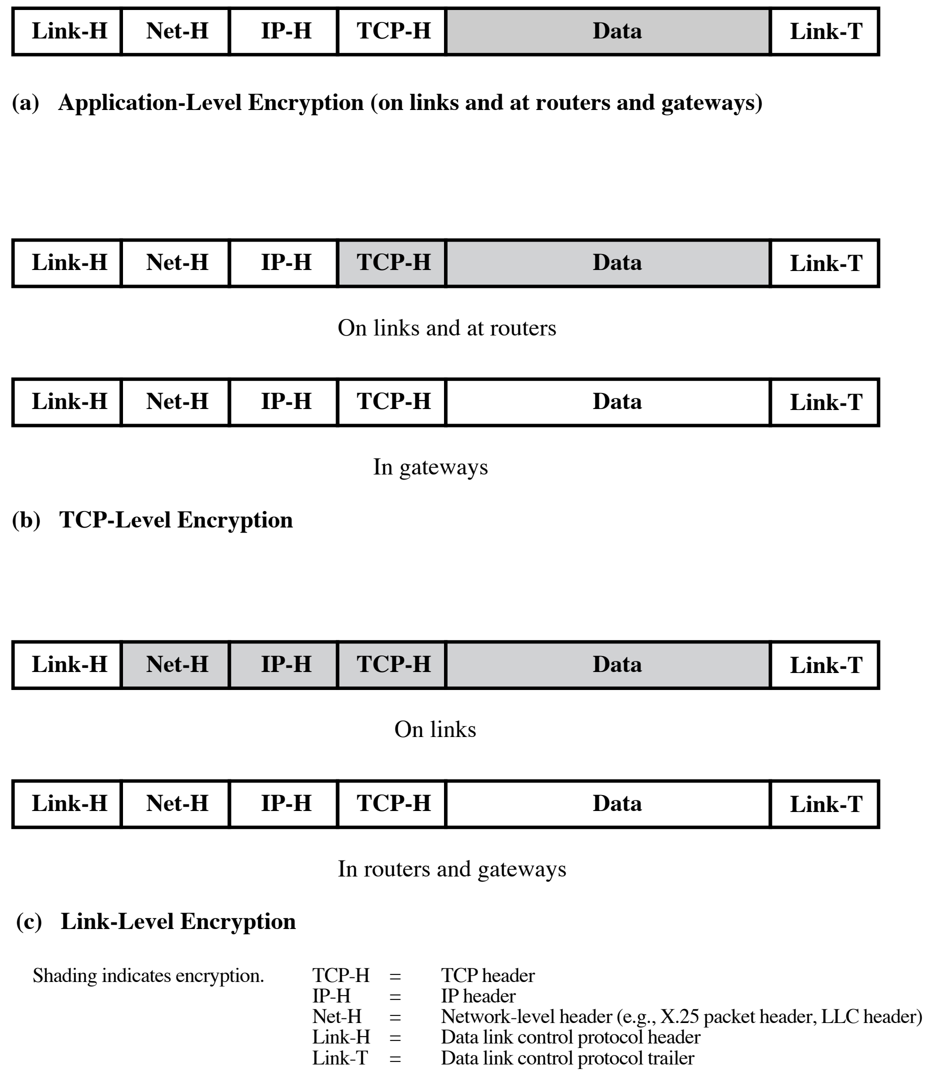
Source: Figure 7.3, Stallings 2006

Store-and-Forward Communications



Source: Figure 7.4, Stallings 2006

Encryption and Protocol Layers



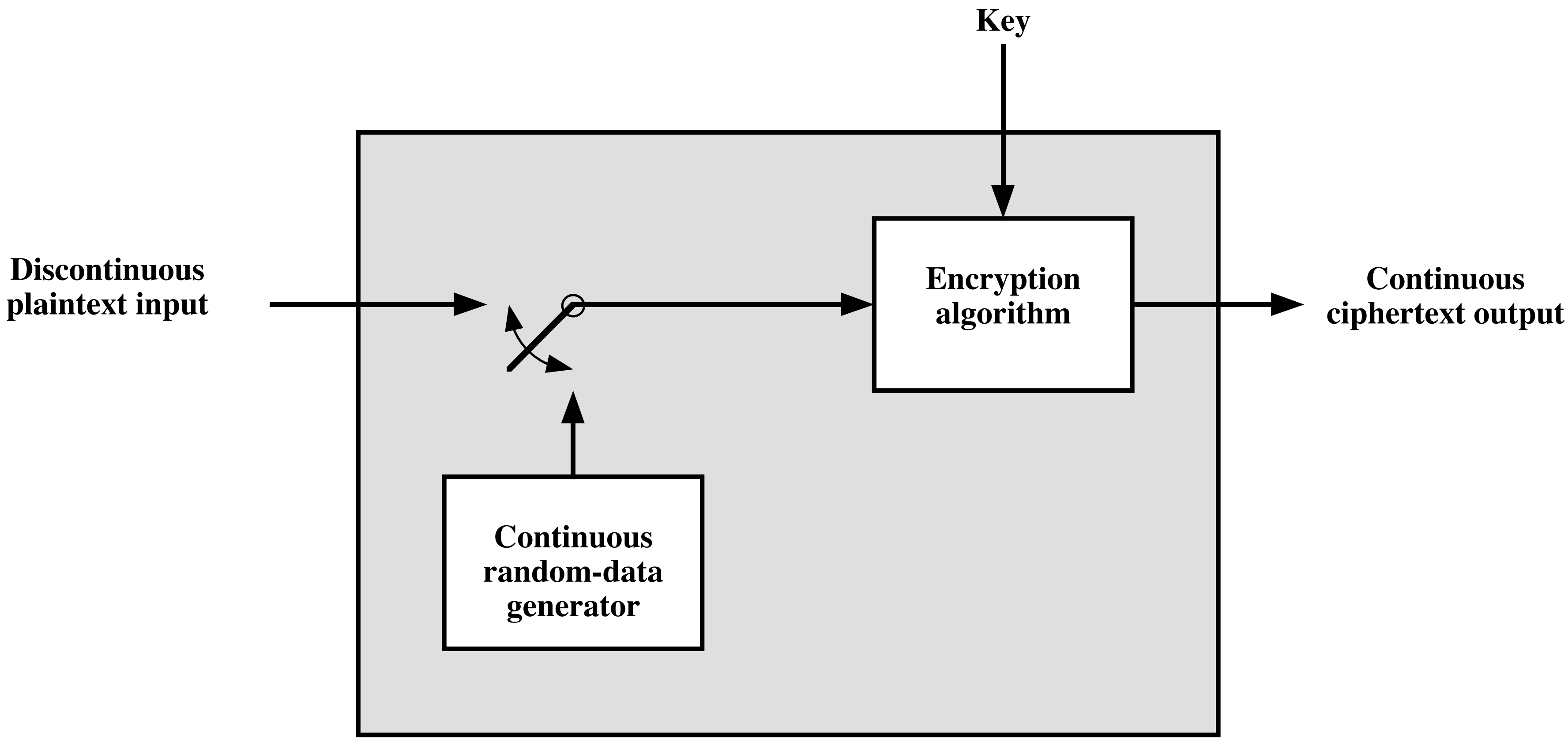
Source: Figure 7.5, Stallings 2006

Traffic Confidentiality

Types of information that can be derived from a traffic analysis attack:

- Identities of partners
- How frequently the partners are communicating
- Message pattern, message length, or quantity of messages
- Events correlated with conversations between particular partners
- Messages of a *covert channel*

Traffic Padding



Source: Figure 7.6, Stallings 2006

Countering Traffic Analysis

- Link encryption approach
  - packet headers already encrypted
  - further strength via traffic padding
- End-to-end encryption approach: available measures more limited
  - padding out data units to a uniform length
  - inserting null messages randomly

The Key Distribution Problem

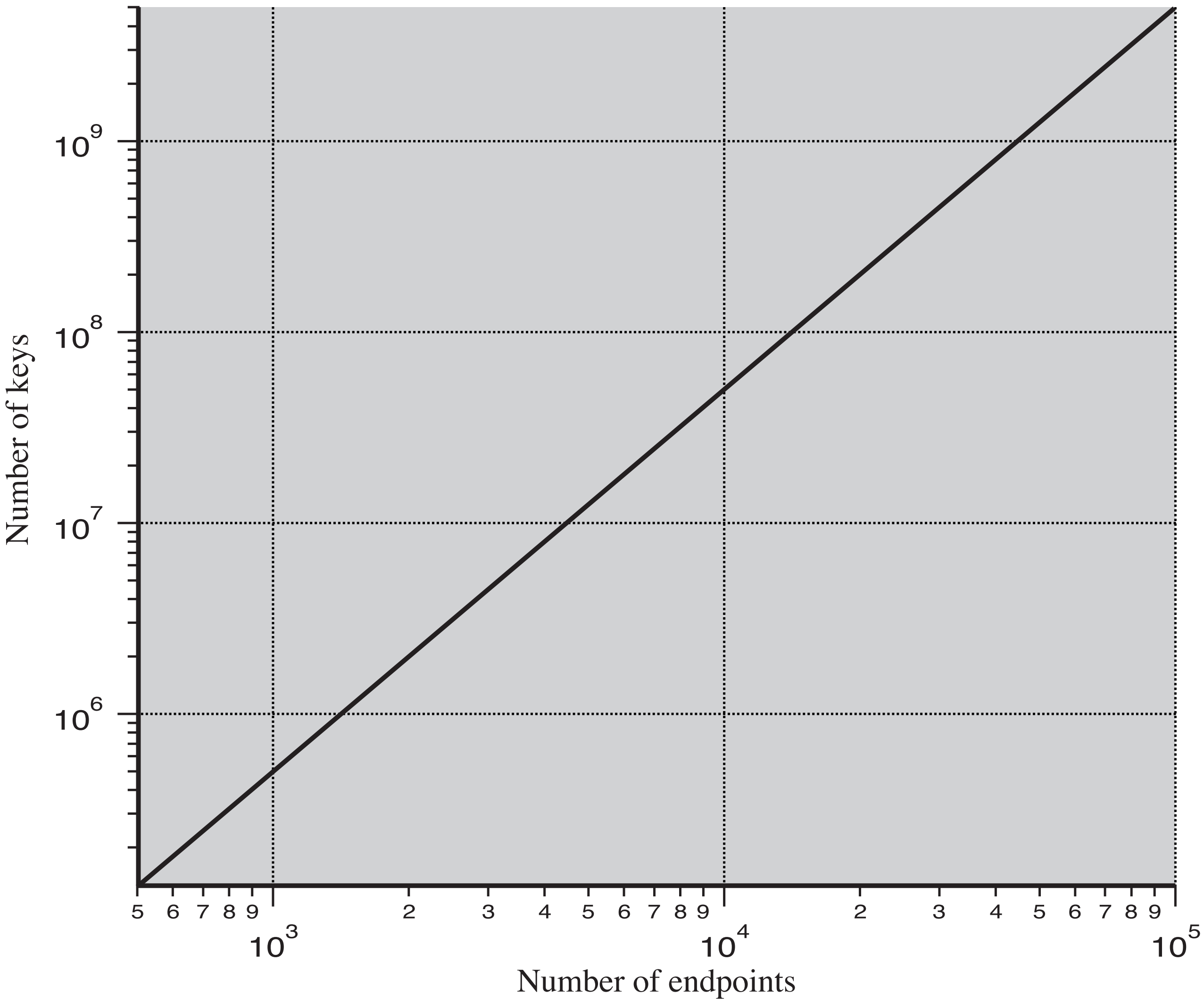
- For symmetric encryption to work, the two parties of an exchange must share the same key and that key must be protected.
- Frequent key changes may be desirable to limit the amount of data compromised.
- The strength of a cryptographic system rests with the technique for solving the key distribution problem—delivering a key to the two parties of an exchange.
- The scale of the problem depends on the number of communication pairs.

Approaches to Key Distribution

Let A (Alice) and B (Bob) be the two parties.

- A key can be selected by A and physically delivered to B.
- A third party can select the key and physically deliver it to A and B.
- If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
- If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B.

Number of Keys for Endpoints

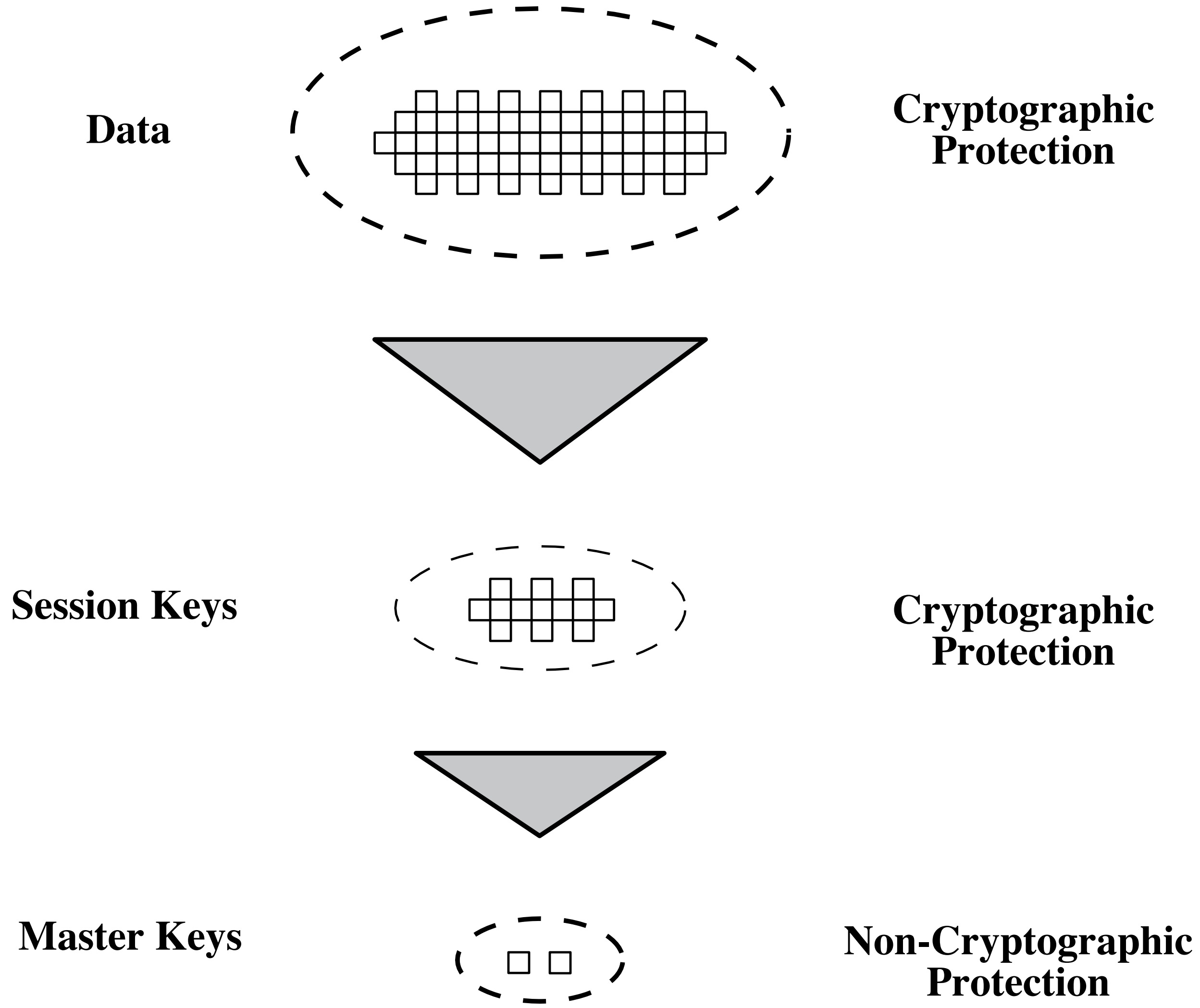


Source: Figure 7.7, Stallings 2006

Using a Key Distribution Center

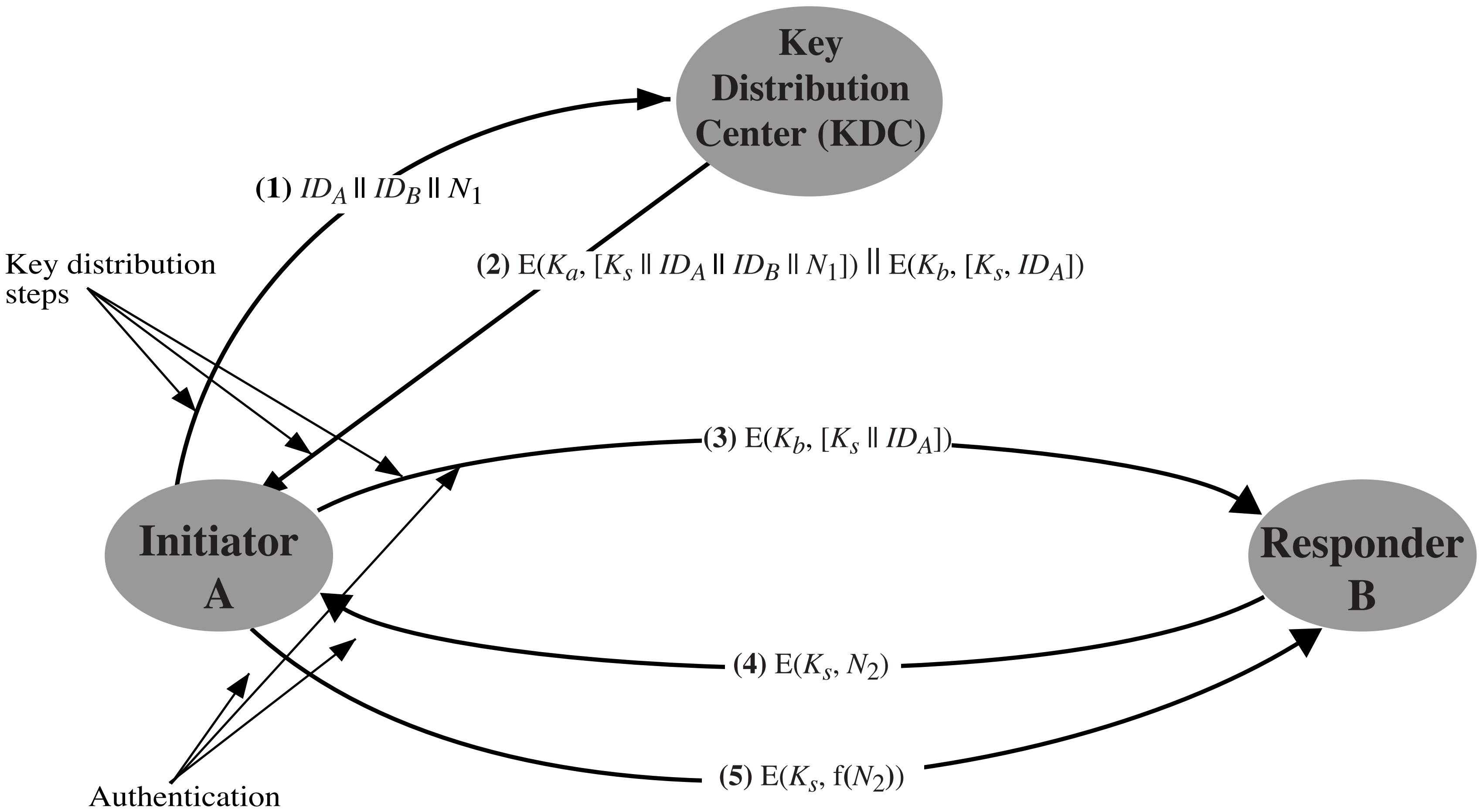
- A key distribution center is responsible for distributing keys to pairs of users as needed.
- Each user must share a unique key with the key distribution center for purposes of key distribution.
- At least two levels of keys must be used: session keys and master keys.
- If there are N end users, $N(N-1)/2$ session keys are needed at any one time, but only N master keys are required.

Key Hierarchy



Source: Figure 7.8, Stallings 2006

Key Distribution Scenario



Source: Figure 7.9, Stallings 2006

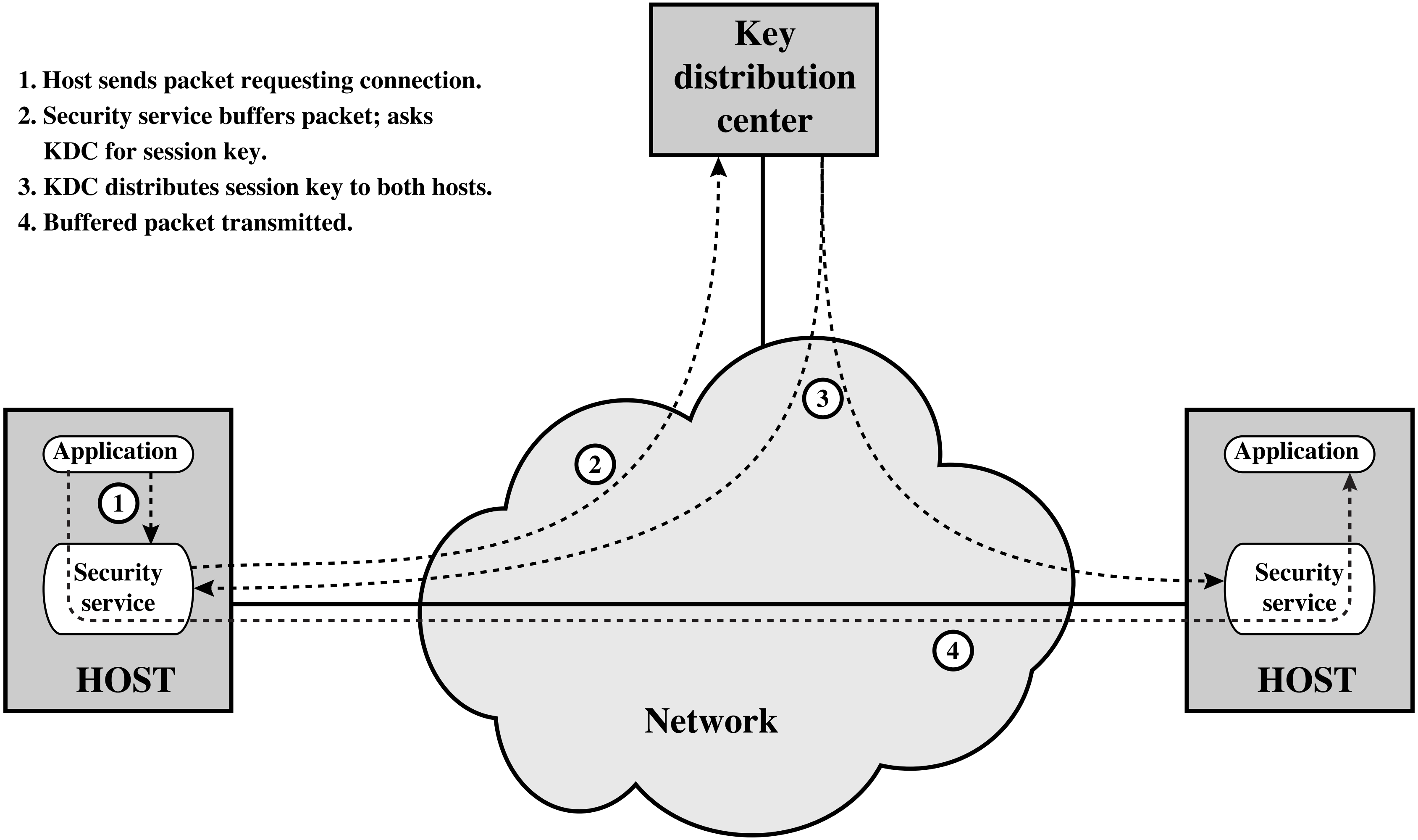
Hierarchical Key Control

- For large networks, a single KDC is inadequate.
- In a hierarchy of KDCs, each local KDC is responsible for a small domain.
- If the two parties are within the same local domain, their KDC is responsible for key distribution.
- Otherwise, the two corresponding local KDCs can communicate through a global KDC. Any of the three KDCs involved can select the key.
- Advantages: distributing the effort of master key distribution and isolating the damage of a fault.

Session Key Lifetime

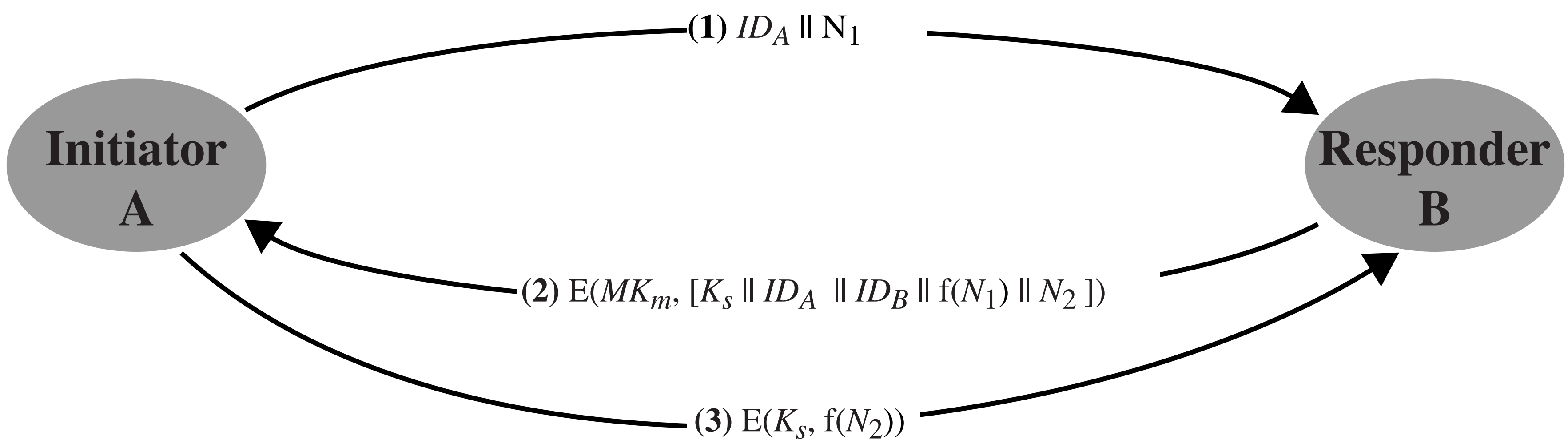
- Two competing considerations in determining the lifetime of a session key:
  - The more frequently session keys are changed, the more secure they are.
  - The distribution of session keys delays the start of an exchange and places a burden on network capacity.
- The decision can be based on whether the communication protocol is connection-oriented or connectionless.

Automatic Key Distribution



Source: Figure 7.10, Stallings 2006

Decentralized Key Distribution



Source: Figure 7.11, Stallings 2006

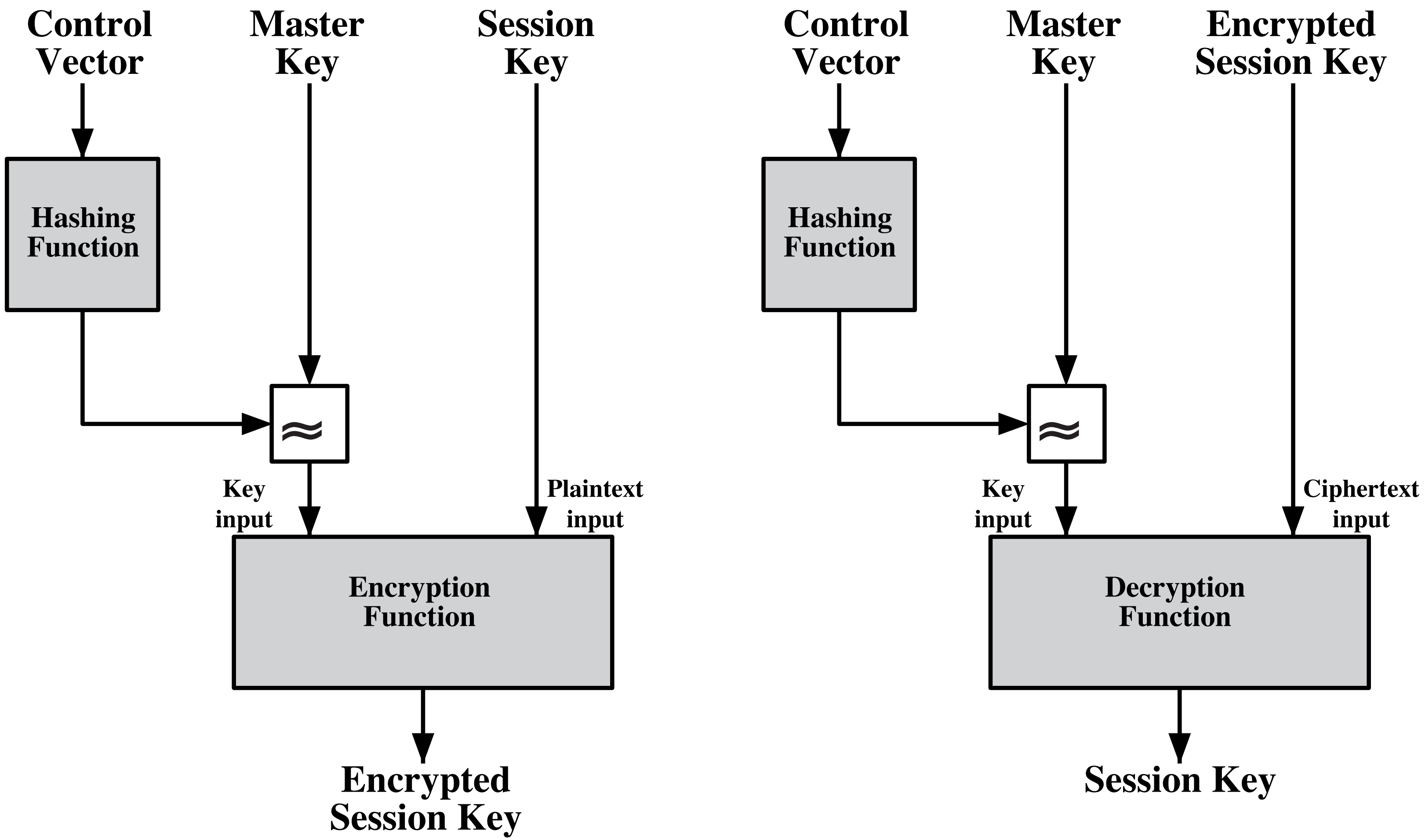
Decentralized Key Control

- The KDC must be trusted and be protected from subversion.
- This requirement can be avoided if the key distribution is fully decentralized.
- A fully decentralized key control, though not feasible for large networks, may be useful within a local context.
- A decentralized approach requires that each end system be able to communicate in a secure manner with all potential partner end systems for purposes of session key distribution.

Controlling Key Usage

- It may be desirable to impose some control on the way in which automatically distributed keys are used.
- Possible types of session keys include: data-encrypting key, PIN-encrypting key, file-encrypting key, etc.
- Key use controlling schemes:
  - Tags
  - Control vectors

Control Vector



(a) Control Vector Encryption

(b) Control Vector Decryption

Source: Figure 7.12, Stallings 2006

The Use of Random Numbers

- Random numbers are used by a number of security algorithms for:
  - Nonces (used in authentication protocols)
  - Session key generation (by the KDC or an end system)
  - Key generation for the RSA algorithm
- Two requirements: randomness and unpredictability.

Pseudorandom Numbers

- True random numbers are hard to come by.
- Cryptographic applications typically use algorithmic techniques for random number generation.
- These algorithms are deterministic and therefore produce sequence of numbers that are not statistically random.
- If the algorithm is good, the resulting sequences will pass reasonable tests for randomness.
- Such numbers are often referred to as pseudorandom numbers.

The Linear Congruential Method

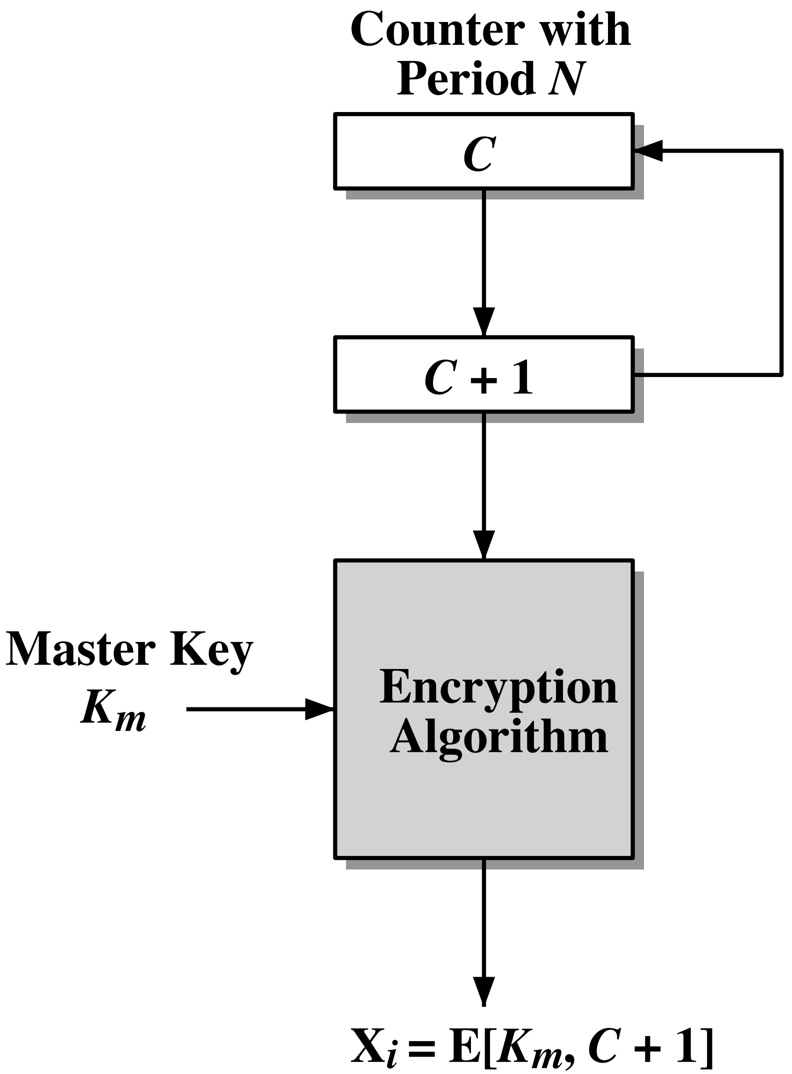
m	the modulus	$m > 0$
a	the multiplier	$0 \le a < m$
c	the increment	$0 \le c < m$
X_0	the starting value (seed)	$0 \le X_0 < m$

- Iterative equation: $X_{n+1} = (aX_n + c) \bmod m$
- Larger values of m imply higher potential for a long period.
- For example, $X_{n+1} = (7^5 X_n) \bmod (2^{31} - 1)$ has a period of $2^{31} - 2$.
- What are the weakness and the remedy?

Cryptographical Generation

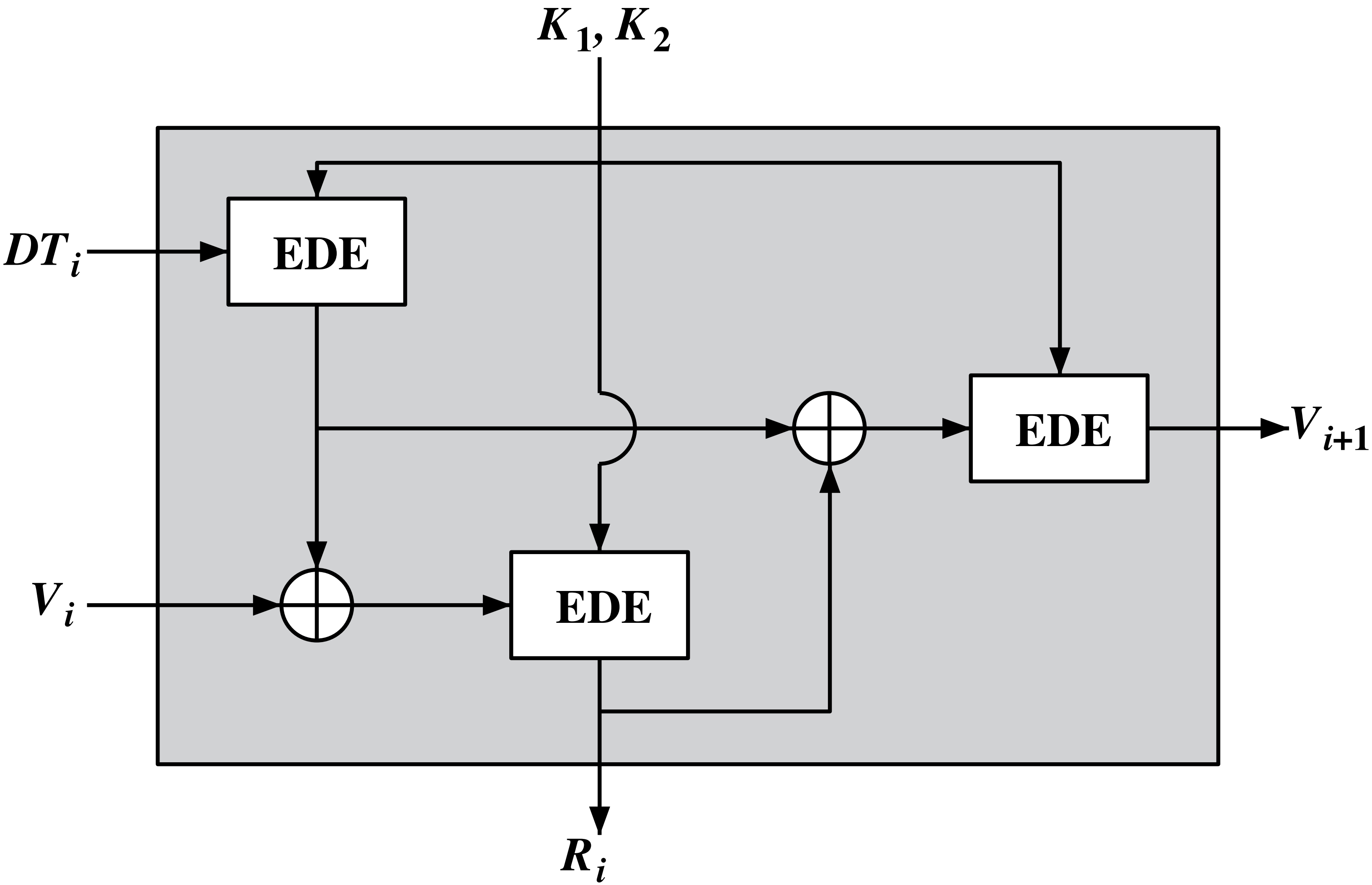
- **Cyclic encryption**: use an arbitrary block cipher. Full-period generating functions are easily obtained.
- **DES Output Feedback Mode**: the successive 64-bit outputs constitute a sequence of pseudorandom numbers.
- **ANSI X9.17 Pseudorandom number generator (PRNG)**: make use of triple DES. Employed in financial security applications and PGP.

Pseudorandom Number Generation



Source: Figure 7.13, Stallings 2006

ANSI X9.17 PRNG



Source: Figure 7.14, Stallings 2006

The Blum Blum Shub (BBS) Generator

- Choose two large prime numbers p and q such that $p \equiv q \equiv 3 \pmod 4$. Let $n = p \times q$.
- Choose a random number s relatively prime to n.
- Bit sequence generating algorithm:

$$X_0 = s^2 \bmod n$$

for $i = 1$ **to** ∞

$$X_i = (X_{i-1})^2 \bmod n$$

$$B_i = X_i \bmod 2$$

- The BBS generator passes the next-bit test.

Example Operation of BBS Generator

i	X_i	B_i
0	20749	
1	143135	1
2	177671	1
3	97048	0
4	89992	0
5	174051	1
6	80649	1
7	45663	1
8	69442	0
9	186894	0
10	177046	0

i	X_i	B_i
11	137922	0
12	123175	1
13	8630	0
14	114386	0
15	14863	1
16	133015	1
17	106065	1
18	45870	0
19	137171	1
20	48060	0

Source: Table 7.2, Stallings 2006