Properties of Secure Network Communication

- **Secrecy:** **Only the sender and intended receiver should be able to understand the contents of the transmitted message.**
  - **Because eavesdroppers may intercept the message, this necessarily requires that the message be somehow encrypted.**
  - **This aspect of secrecy is probably the most commonly perceived meaning of the term "secure communication."**
- **Authentication:** **Both the sender and receiver need to confirm the identity of the other party involved in the communication - to confirm that the other party is indeed who or what they claim to be.**
  - **Most common authentication method used : password protection. Other: using Public key encryption, Secure sockets layer (SSL).**
- **Message Integrity:** **Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either maliciously or by accident, in transmission (e.g. using CRCs).**

Network Security: Traditional Encryption

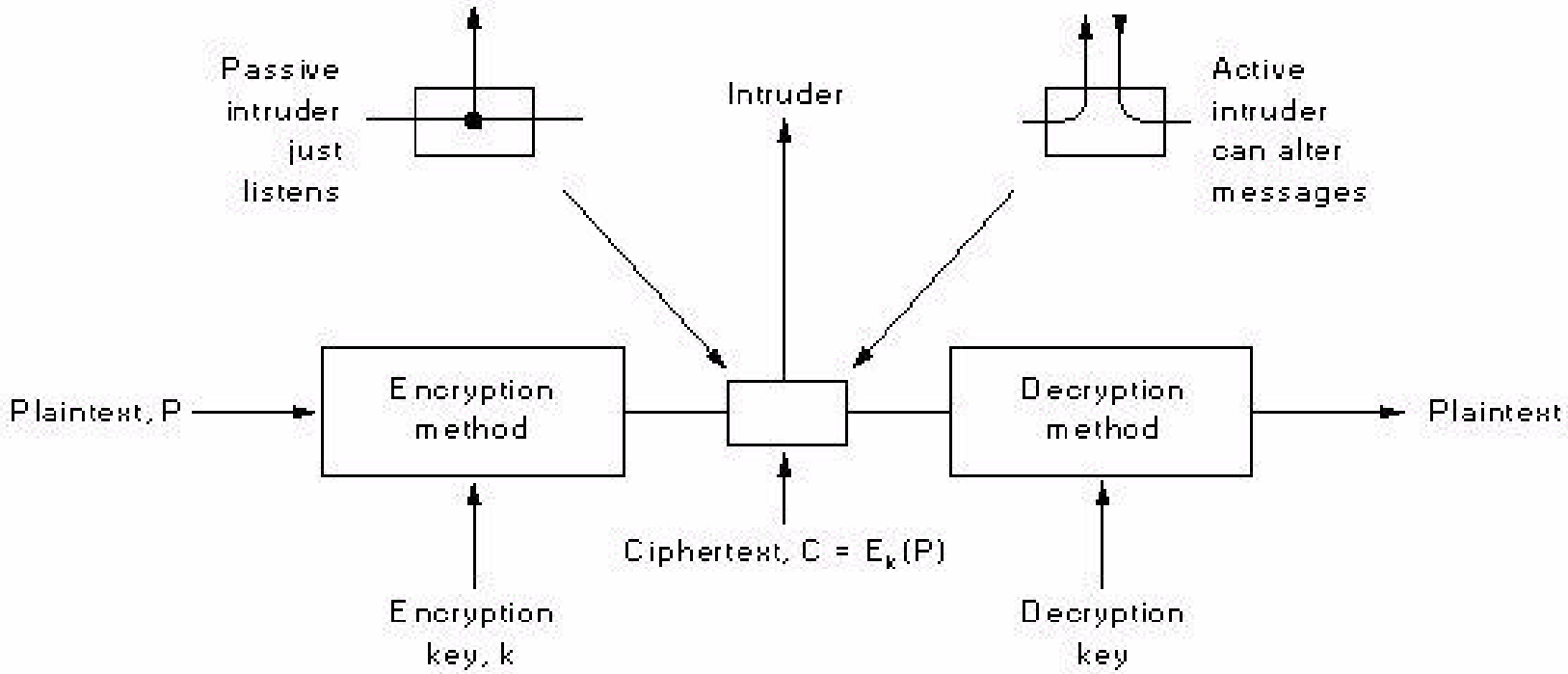
Plaintext P: Messages to be encrypted.

Key K: Parameter of encryption function. If the key is a binary number then a longer key indicates a stronger cipher.

E_k: Encryption Algorithm.

Ciphertext C: The encrypted message. $C = E_K(P)$

D_k: Decryption Algorithm. $P = D_K(C) = D_K(E_K(P))$



Basic Cipher Types

- **Substitution Ciphers:** **Replace each letter by a different letter:**

  Example: Caesar cipher, monoalphabetic substitution

  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: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

- **Transposition Ciphers:** **Letters reordered.**

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext

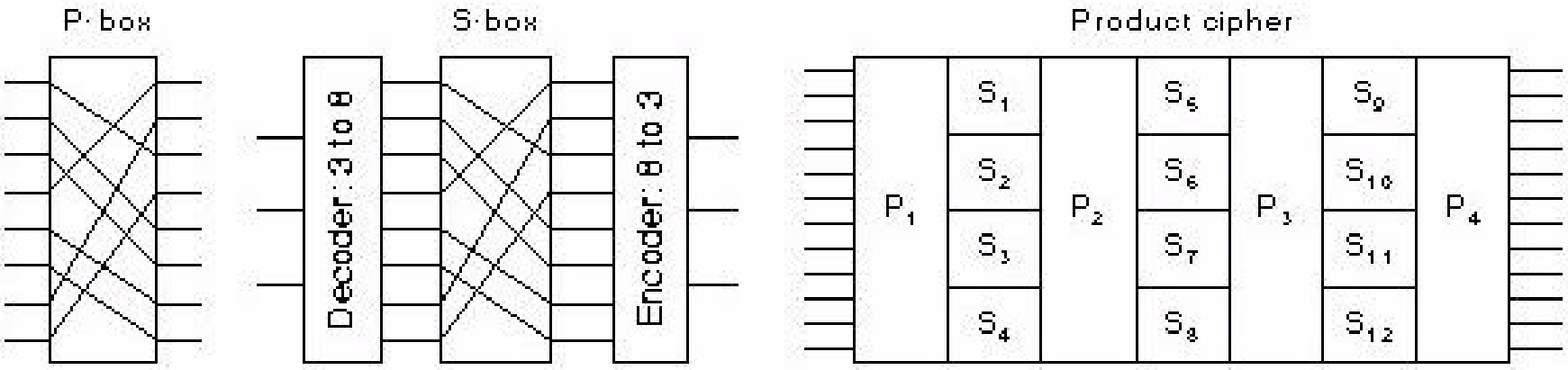
pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Secret-Key Encryption Algorithms

- **Complex encryption algorithms that rely on series of transpositions and substations.**
- **P-box: Performs a specific permutation on input characters/bits.**
- **S-box: Performs a specific substitution on input character/bits.**
- **Product cipher: Encryption using a series of P and S boxes.**

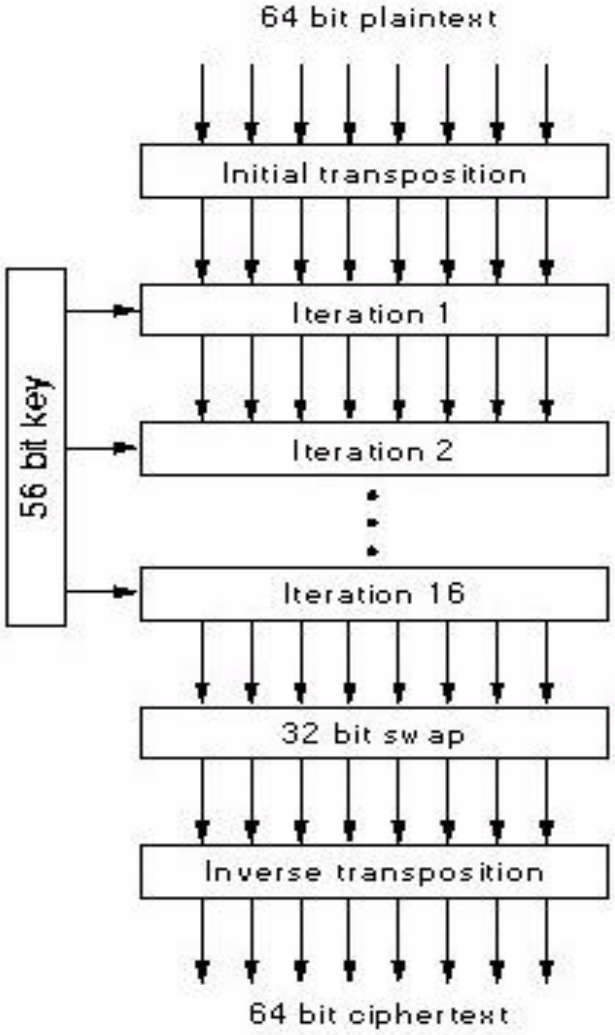


Data Encryption Standard (DES)

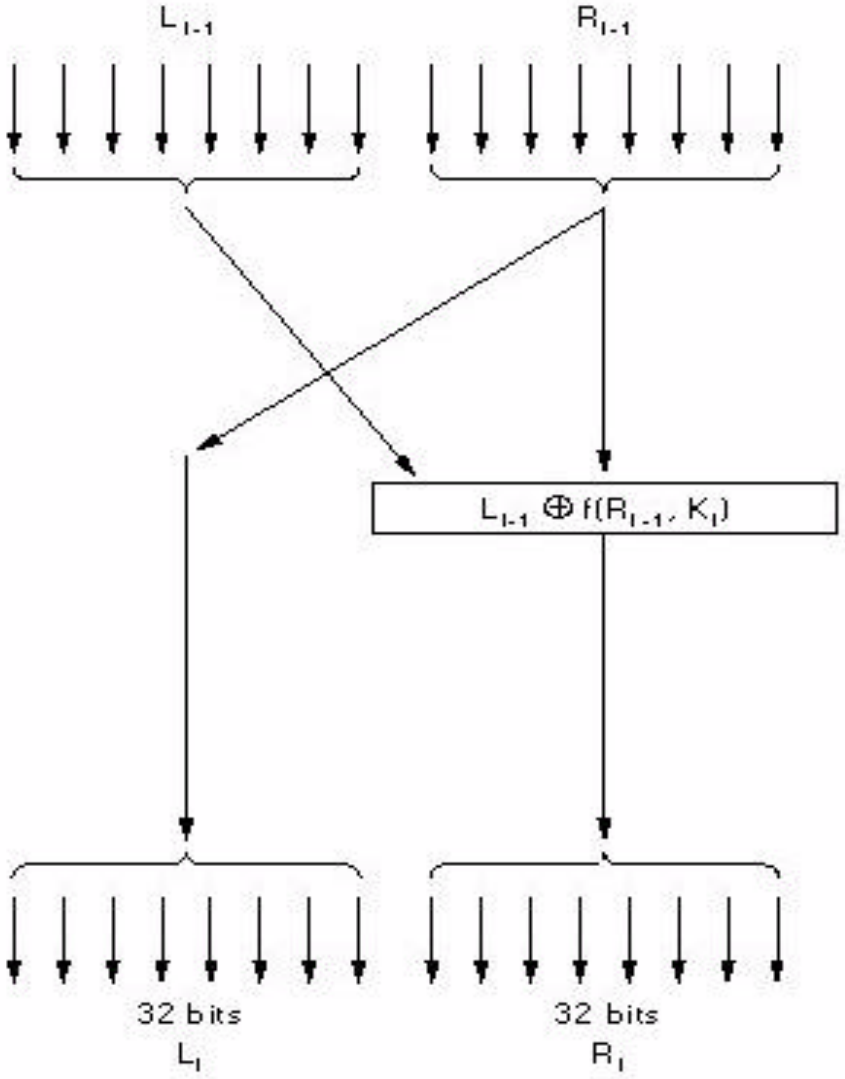
- **Data Encryption Standard (DES), is a symmetric key encryption standard published in 1977 by the US National Bureau of Standards for commercial and non-classified US government use.**
- **DES encodes plaintext in 64 bit chunks using a 64-bit key. Actually, 8 of these 64 bits are odd parity bits (one bit for each of the 8 bytes), so the DES key is effectively 56 bits long.**
- **DES consists of two permutation P-box steps (the first and last steps of the algorithm) in which all 64 bits are permuted, and 16 identical "rounds" of operation in between.**
- **During each round, the rightmost 32 bits of the input are moved to the left 32 bits of the output. The entire 64-bit input to the ith round and the 48 bit key for the ith round (derived from the larger DES 56-bit) are taken as input to a function that involves expansion of four-bit input chunks into six-bit chunks, exclusive OR-ing with the expanded six bit chunks of the 48-bit key Ki, a substitution operation and further exclusive OR-ing with the leftmost 32 bits of the input; The resulting 32-bit output of the function is then used as the rightmost 32 bits of the rounds 64-bit output.**
- **Decryption works by reversing the algorithm's operations.**

DES Steps

64-bit blocks of plain text encrypted in 19 stages into 64-bit blocks of ciphertext



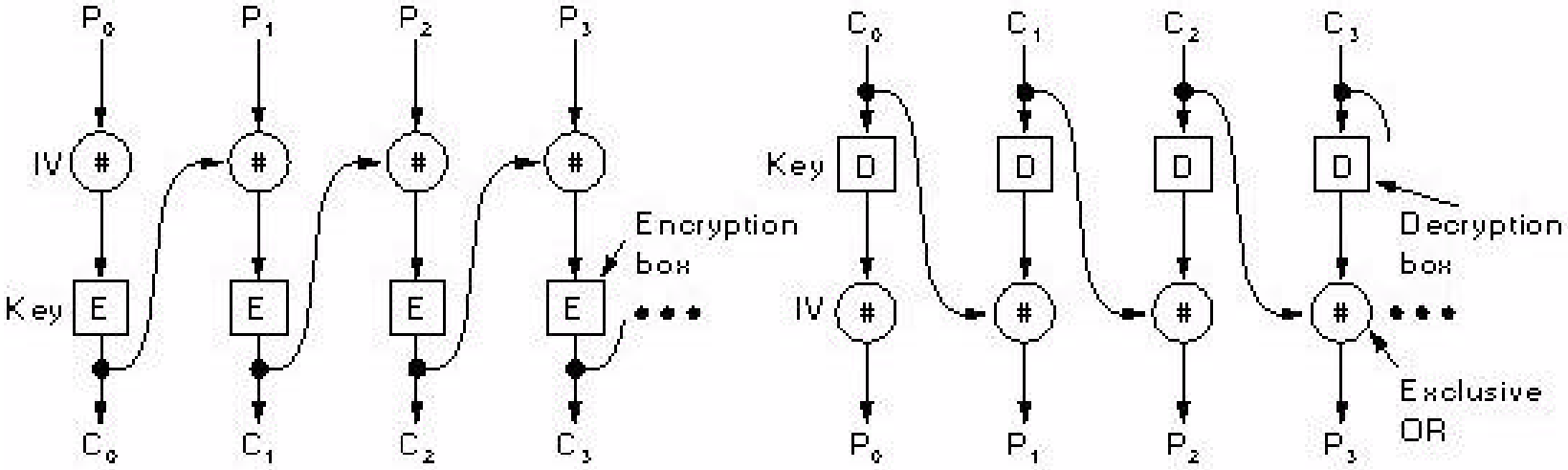
DES General Outline



Detail of One Iteration Stage

Cipher-Block Chaining

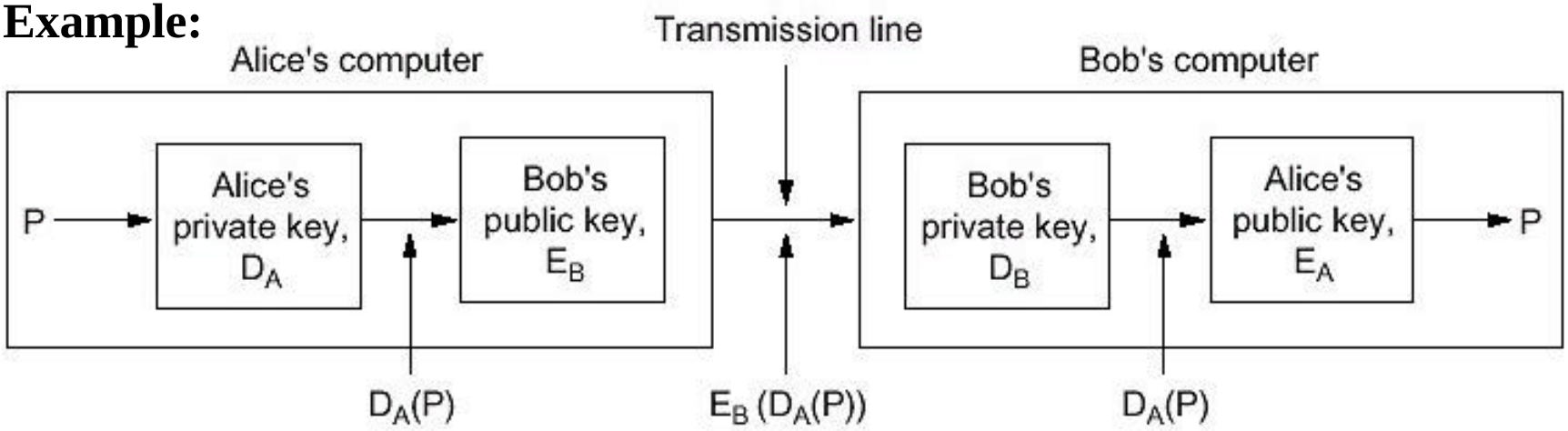
When longer messages than 64 bits are encrypted in DES, which is typically the case, a technique known as cipher-block chaining is used, in which the encrypted version of the jth 64-bit quantity of data is XOR'ed with the (j+1)st unit of data before the (j+1)st unit of data is encrypted.



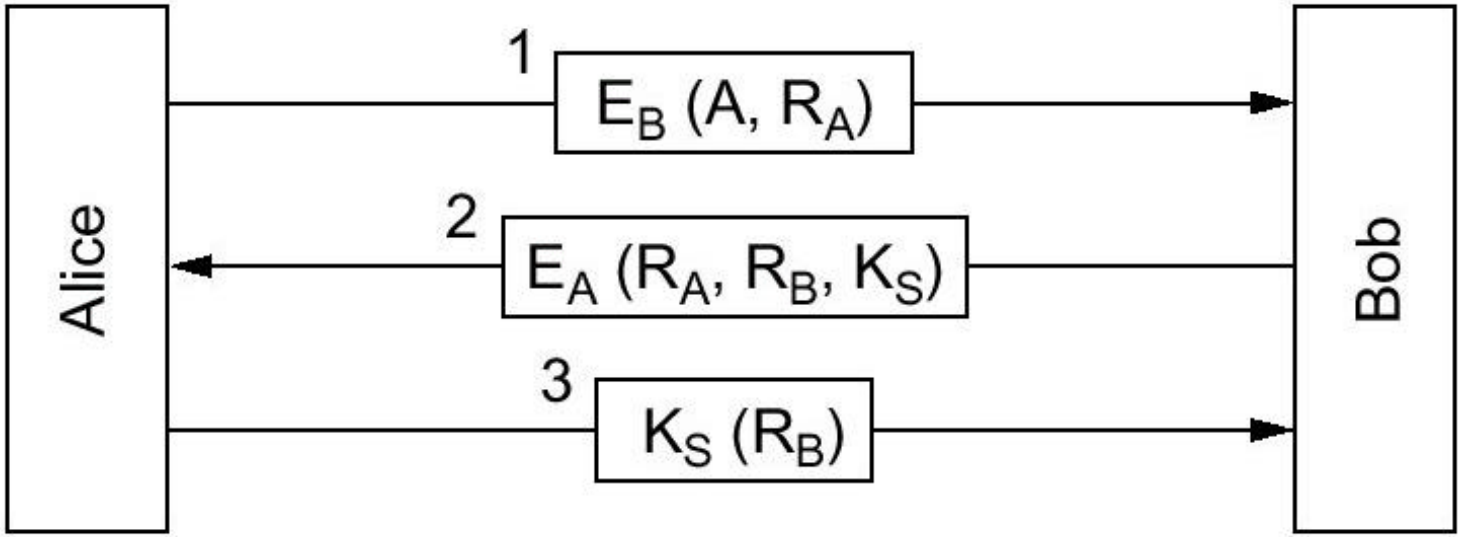
Public Key Encryption

- **Encryption and decryption keys are different:**
  - **Public key is known and made public.**
  - **Private key secret and is held by owner.**
- **To encrypt a message: The recipient's public key along with the sender's private key are used.**
- **To decrypt a message the receiver's private key along with the sender's public key are used.**
- **Digital Signature: Encrypt using private key of user. Decrypt using public key. Only owner of private key could have generated original message.**
- **Example Algorithm: The RSA (Rivest, Shamir, Adleman) Algorithm.**

Example:



Mutual Authentication Using Public Key Encryption



Internet Security:

Secure sockets layer (SSL)

- **Originally developed by Netscape, SSL is a protocol designed to provide data encryption and authentication between a Web client and a Web server.**
- **The protocol begins with a handshake phase that negotiates an encryption algorithm (e.g., DES) and encryption keys, authenticating the server to the client.**
- **Optionally, the client can also be authenticated to the server.**
- **Once the handshake is complete and the transmission of application data begins, all data is encrypted using session keys negotiated during the handshake phase.**
- **SSL is widely used in Internet commerce, being implemented in almost all popular browsers and Web servers. It is also the basis of the Transport Layer Security (TLS) protocol [RFC 2246].**

SSL Features

- **SSL server authentication, allowing a user to confirm a server's identity. An SSL enabled browser maintains a list of trusted certifying authorities (CAs) along with the public keys of the CAs.**
- **When the browser wants to do business with an SSL-enabled Web server, the browser obtains from the server a certificate containing the server's public key. The certificate is issued (i.e., digitally signed) by a certificate authority (CA) listed in the client's list of trusted CAs.**
  - **This feature allows the browser to authenticate the server before the user submits a payment card number.**
- **An encrypted SSL session, in which all information sent between browser and server is encrypted by sending software (browser or Web server) and decrypted by the receiving software (browser or Web server).**
- **SSL client authentication, allowing a server to confirm a user's identity. Analogous to server authentication, client authentication makes use of client certificates, which have also been issued by CAs.**

SSL Handshake Steps

1. The browser sends the server the browser's SSL version number and cryptography preferences.
2. The server sends the browser the server's SSL version number, cryptography preferences and its certificate. The certificate includes the server's RSA public key and is certified by some CA, that is, the certificate has been encrypted by a CA's private key.
3. When the browser receives the certificate from the server, it checks to see if the CA is on the entrusted list of CAs . If not, the user is warned of the problem and idicates that an encrypted and authenticated connection cannot be established. If yes, the browser uses the CA's public key to decrypt the certificate and obtain the server's public key.
4. The browser generates a symmetric session key, encrypts it with the server's public key, and sends the encrypted session key to the server.
5. The browser sends a message to the server informing it that future messages from the client will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the browser portion of the handshake is finished.
6. The server sends a message to the browser informing it that future messages from the server will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the server portion of the handshake is finished.
7. The SSL handshake is now complete, and the SSL session has begun. The browser and the server use the session key to encrypt and decrypt the data they send to each other and to validate its integrity.