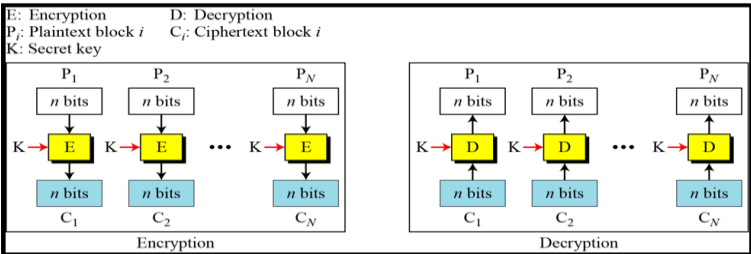
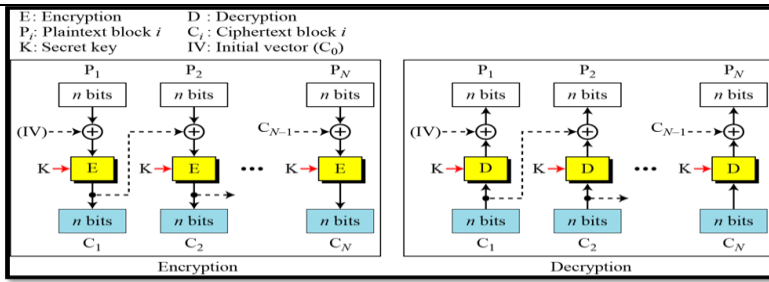


Internal Assessment Test – II Solution and Scheme of Evaluation

Sub:	NETWORK SECURITY	Sec	A & B				Code:	10EC832	
Date:	17 / 04 / 2018	Duration:	90 mins	Max Marks:	50	Sem:	VIII	Branch:	TCE

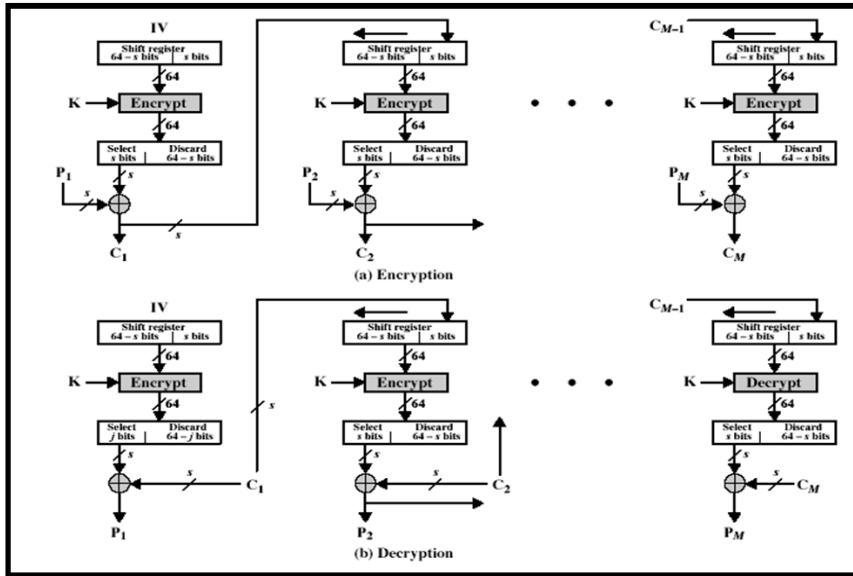
Note: Answer any five full questions.

		Marks	OBE	
			CO	RB T
			CO2	L2
1	<p>Describe the block cipher modes of operation in detail</p> <p>BLOCK CIPHER MODES OF OPEARTION: If data is more than 64 bits, e.g. we have 1Mbyte files and we want to encrypt it, then we will break the files into block and encrypt each block at a time and then each block will be combined together. We may perform padding if necessary (either we will fill it with zero or we may repeat the same plain text). There are different modes of operation to perform it.</p> <ol style="list-style-type: none"> a) Electronic Code Book (ECB) b) Cipher Block Chaining Mode (CBC) c) Cipher Feedback Mode (CFB) d) Output Feedback Mode(OFB) e) Counter Mode <p>Electronic Code Book (ECB):</p> <p>The encryption algorithm is represented as $C_i = E_K(P_i)$</p> <p>The decryption algorithm is represented as $P_i = D_K(C_i)$</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>E: Encryption D: Decryption P_i: Plaintext block i C_i: Ciphertext block i K: Secret key</p>  </div> <p>Cipher Feedback Mode: (CFB)</p> <p>The encryption algorithm is represented as $C_j = E_K[C_{j-1} \oplus P_j]$</p> <p>The decryption algorithm is represented as $P_j = C_{j-1} \oplus D_K[C_j]$</p>	10		
		2 X 5		

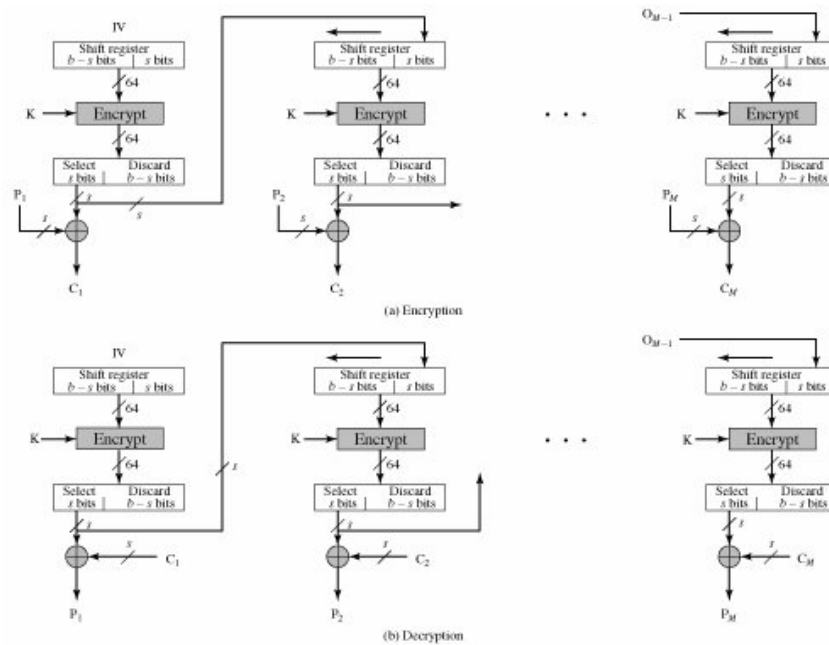


Cipher Feedback Mode: (CFB)

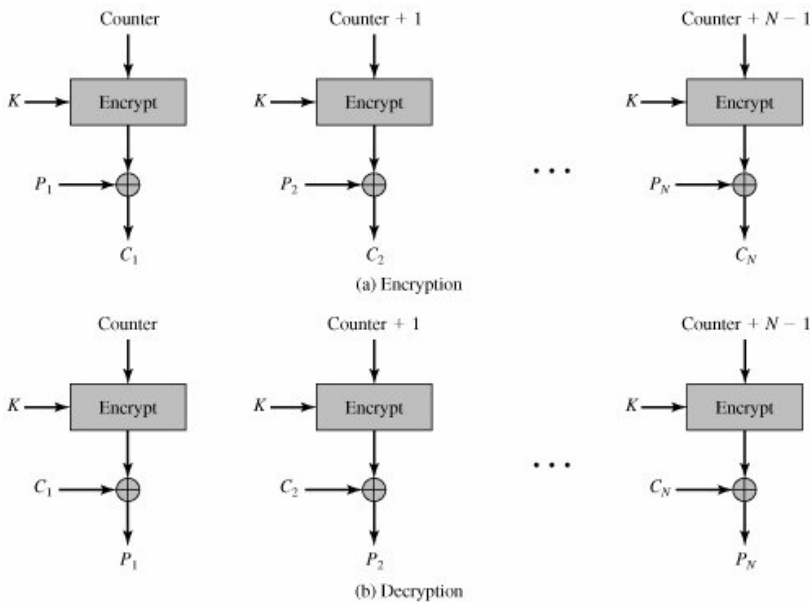
$$C_1 = P_1 \oplus S_S(E_K(IV)) \text{ and } P_1 = C_1 \oplus S_S(E_K(IV))$$



Output Feedback Mode: (OFB)



Counter Mode: (CTR):



2 (a) Discuss the final evaluation criteria of AES

5

General Security:

Rijndael has no known security attacks. Rijndael uses S-boxes as nonlinear components. Rijndael appears to have an adequate security margin, but has received some criticism suggesting that its mathematical structure may lead to attacks. On the other hand, the simple structure may have facilitated its security analysis during the timeframe of the AES development process.

Software Implementations:

Rijndael performs encryption and decryption very well across a variety of platforms, including 8-bit and 64-bit platforms, and DSPs. However, there is a decrease in performance with the higher key sizes because of the increased number of rounds that are performed. Rijndael's high inherent parallelism facilitates the efficient use of processor resources, resulting in very good software performance even when implemented in a mode not capable of interleaving. Rijndael's key setup time is fast.

5

Restricted-Space Environments:

In general, Rijndael is very well suited for restricted-space environments where either encryption or decryption is implemented (but not both). It has very low RAM and ROM requirements. A drawback is that ROM requirements will increase if both encryption and decryption are implemented simultaneously, although it appears to remain suitable for these environments. The key schedule for decryption is separate from encryption.

Hardware Implementations:

Rijndael has the highest throughput of any of the finalists for feedback modes and second highest for non-feedback modes. For the 192 and 256-bit key sizes, throughput falls in standard and unrolled implementations because of the additional number of rounds. For fully pipelined implementations, the area requirement increases, but the throughput is unaffected.

(b) Explain block cipher design principles

5

Three critical aspects of block cipher design:

- a) The number of rounds
- b) Design of the function F
- c) Key scheduling.

5

DES Design Criteria

	CO2	L2
	CO2	L4

The criteria used in the design of DES, focused on the design of the S-boxes and on the P function that takes the output of the S boxes the S-boxes are the only nonlinear part of DES. If the S-boxes were linear the entire algorithm would be linear and easily broken. The P-boxes are used to increase the diffusion of the algorithm.

a) Number of Rounds

The greater the number of rounds, the more difficult it is to perform cryptanalysis, even for a relatively weak F. In general, the criterion should be that the number of rounds is chosen so that known cryptanalytic efforts require greater effort than a simple brute-force key search attack. This criterion was certainly used in the design of DES. This criterion is attractive because it makes it easy to judge the strength of an algorithm and to compare different algorithms.

b) Design of Function F

The function F provides the element of confusion in a Feistel cipher. Thus, it must be difficult to "unscramble" the substitution performed by F. One obvious criterion is that F be nonlinear. The more nonlinear F, the more difficult any type of cryptanalysis will be. The algorithm should have good avalanche properties. This means that a change in one bit of the input should produce a change in many bits of the output.

A more stringent version of this is the **strict avalanche criterion (SAC)**, which states that any output bit j of an S-box should change with probability $1/2$ when any single input bit i is inverted for all i, j .

Another criterion is the **bit independence criterion (BIC)**, which states that output bits j and k should change independently when any single input bit i is inverted, for all i, j , and k .

The SAC and BIC criteria appear to strengthen the effectiveness of the confusion function.

c) Key Schedule Algorithm

The key is used to generate one subkey for each round. In general, we would like to select subkeys to maximize the difficulty of deducing individual subkeys and the difficulty of working back to the main key.

The key schedule should guarantee Strict Avalanche Criterion and Bit Independence Criterion.

3 List different types of threats and consequences when using the web. Also list countermeasure to be taken

10

C06

L1

	Threats	Consequences	Countermeasures
Integrity	<ul style="list-style-type: none"> •Modification of user data •Trojan horse browser •Modification of memory •Modification of message traffic in transit 	<ul style="list-style-type: none"> •Loss of information •Compromise of machine •Vulnerability to all other threats 	Cryptographic checksums
Confidentiality	<ul style="list-style-type: none"> •Eavesdropping on the net •Theft of info from server •Theft of data from client •Info about network configuration •Info about which client talks to server 	<ul style="list-style-type: none"> •Loss of information •Loss of privacy 	Encryption, Web proxies
Denial of Service	<ul style="list-style-type: none"> •Killing of user threads •Flooding machine with bogus requests •Filling up disk or memory •Isolating machine by DNS attacks 	<ul style="list-style-type: none"> •Disruptive •Annoying •Prevent user from getting work done 	Difficult to prevent
Authentication	<ul style="list-style-type: none"> •Impersonation of legitimate users •Data forgery 	<ul style="list-style-type: none"> •Misrepresentation of user •Belief that false information is valid 	Cryptographic techniques

A Comparison of Threats on the Web

10

4 Explain various phases of SSL handshake protocols

10

C06

L4

HANDSHAKE PROTOCOL: The handshake protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and the keys to be used to protect data sent in an SSL record. The handshake protocol is used before any application data is transmitted. The handshake protocol consists of a series of messages exchanged by client and server. Each message has 3 fields

- Type(1 Byte)
- Length (3 Bytes)
- Content (≥ 0 Bytes)



Handshake Protocol

- Handshake is done in 4 phases.

Phase -1: (Establishing security capabilities):

This phase is used to initiate a logical connection. This exchange is initiated by the client, which sends a client hello message with the following parameters.

Version, Client random number, Session ID, Cipher Suite, Compression Method.

After sending the client hello message, the client waits for the server-hello message, the server hello message has the following parameters.

Version, Server random number, Session ID, Selected cipher set, Selected compression method.

After phase 1, the client and server know the following:

The version of SSL, The algorithm for key exchange, message authentication and encryption, The compression method, The 2 random numbers for key generation.

5(Diagram)+
5(Explanation)

Phase-2: (Server key exchange and authentication):

The server begins this phase by sending its certificates. At the end, the server announces that the server hello process is done. The phase 2 has these 4 following steps.

Certificate, Server key exchange, Certificate request, Server Hello Done

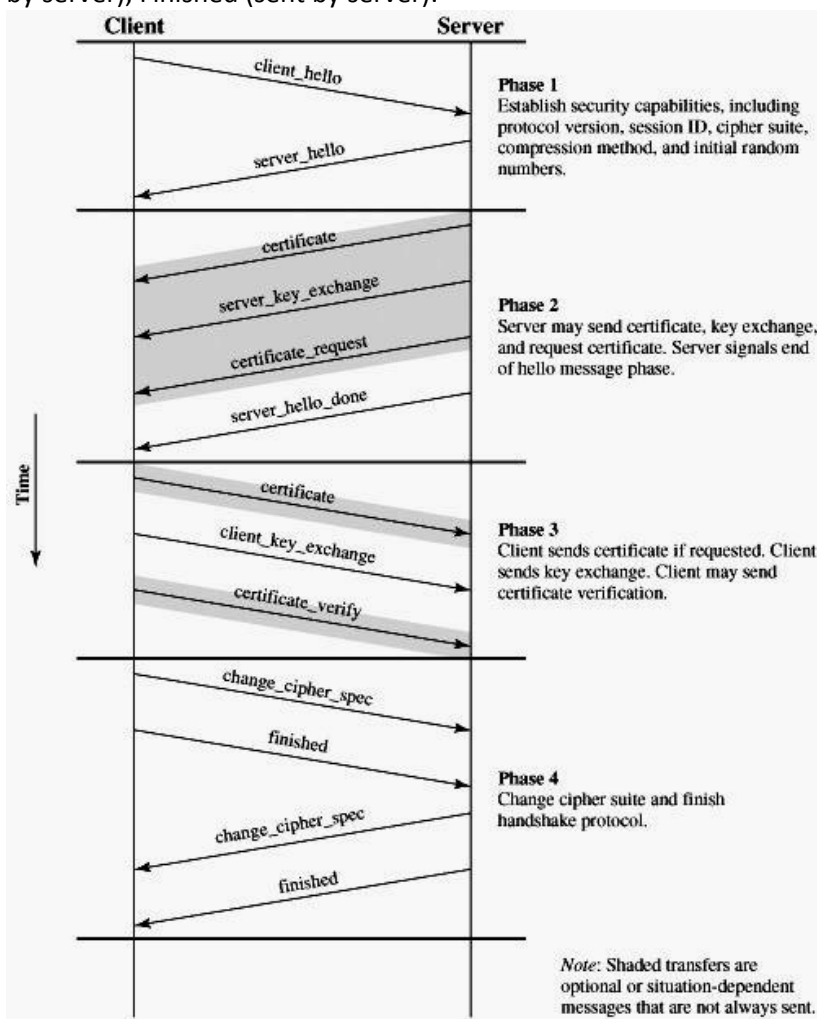
After phase 2, the server is authenticated to the client and the client knows the public key of the server if required.

Phase-3: (Client key exchange and authentication)

Phase-3 is designed to authenticate the client. In this phase, 3 messages can be sent from the client to the server. Those are Certificate, Client Key exchange, Certificate verifies. After phase 3, The client is authenticated for the server and Both the client and the server knows the pre-master secret.

Phase-4: (Finalizing and Finishing)

In phase 4, the client and server send messages to change cipher specification and to finish the handshaking protocols. In this phase, 4 messages are exchanged those are Change cipher spec (sent by client), Finished (sent by client), Change cipher spec (sent by server), Finished (sent by server).



5 Who are the participants of SET? Give the sequence of events required for SET. Explain with appropriate diagram.

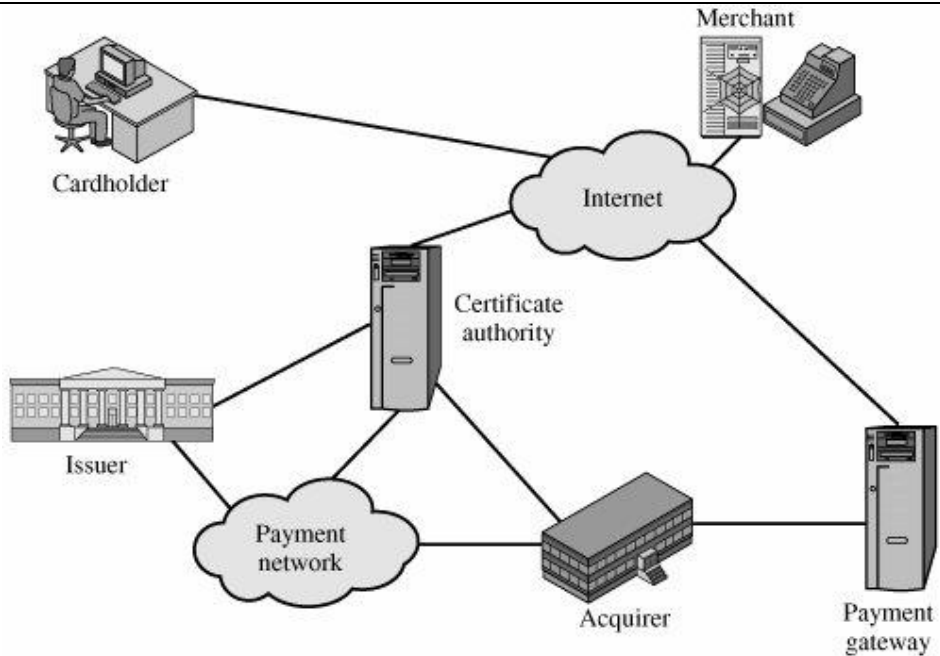
SET Participants:

10

C06

L4

5(Diagram)+
5(Expl)



[Figure: Secure Electronic Commerce Components]

- a) **Cardholder:** In the electronic environment, consumers and corporate purchasers interact with merchants from personal computers over the Internet. A cardholder is an authorized holder of a payment card (e.g., MasterCard, Visa) that has been issued by an issuer.
- b) **Merchant:** A merchant is a person or organization that has goods or services to sell to the cardholder. Typically, these goods and services are offered via a Web site or by electronic mail. A merchant that accepts payment cards must have a relationship with an acquirer.
- c) **Issuer:** This is a financial institution, such as a bank, that provides the cardholder with the payment card. Typically, accounts are applied for and opened by mail or in person. Ultimately, it is the issuer that is responsible for the payment of the debt of the cardholder.
- d) **Acquirer:** This is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments. Merchants will usually accept more than one credit card brand but do not want to deal with multiple bankcard associations or with multiple individual issuers. The acquirer provides authorization to the merchant that a given card accounts is active and that the proposed purchase does not exceed the credit limit. The acquirer also provides electronic transfer of payments to the merchant's account. Subsequently, the acquirer is reimbursed by the issuer over some sort of payment network for electronic funds transfer.
- e) **Payment gateway:** This is a function operated by the acquirer or a designated third party that processes merchant payment messages. The payment gateway interfaces between SET and the existing bankcard payment networks for

authorization and payment functions. The merchant exchanges SET messages with the payment gateway over the Internet, while the payment gateway has some direct or network connection to the acquirer's financial processing system.

- f) **Certification authority (CA):** This is an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways. The success of SET will depend on the existence of a CA infrastructure available for this purpose. As was discussed in previous chapters, a hierarchy of CAs is used, so that participants need not be directly certified by a root authority.

SEQUENCE OF EVENTS

- 1) **The customer opens an account**
- 2) **The customer receives a certificate**
- 3) **Merchants have their own certificates**
- 4) **The customer places an order**
- 5) **The merchant is verified**
- 6) **The order and payment are sent**
- 7) **The merchant requests payment authorization**
- 8) **The merchant confirms the order**
- 9) **The merchant provides the goods or service**
- 10) **The merchant requests payment.**

6 What are the different types of intrusion detection system and explain it?

10

C06	L2
-----	----

Intrusion Detection

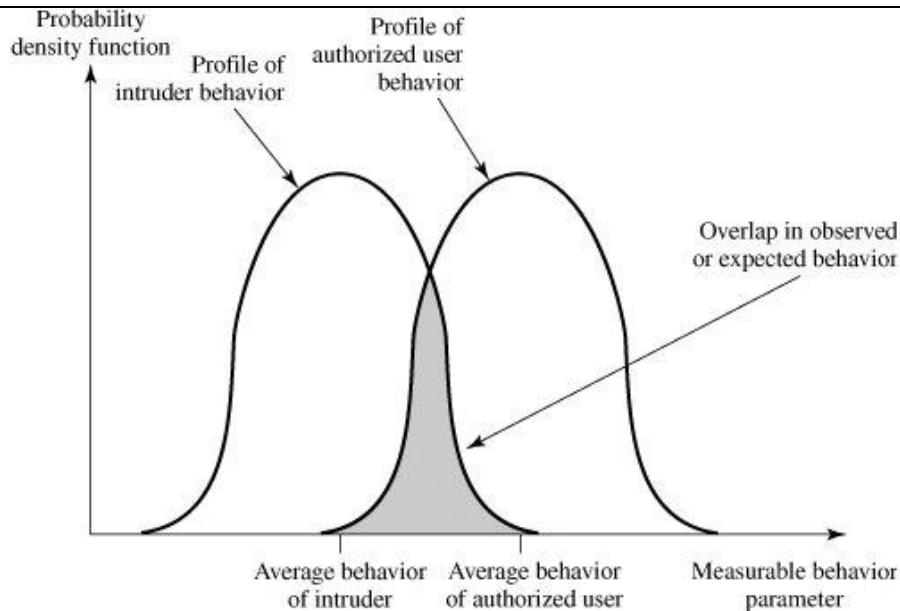
Intrusion Detection is required for the following reason:

1. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.
2. An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions.
3. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

Intrusion detection is based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified. Of course, we cannot expect that there will be a crisp, exact distinction between an attack by an intruder and the normal use of resources by an authorized user. Rather, we must expect that there will be some overlap.

The nature of the task confronting the designer of an intrusion detection system. Although the typical behavior of an intruder differs from the typical behavior of an authorized user, there is an overlap in these behaviors. Thus, a loose interpretation of intruder behavior, which will catch more intruders, will also lead to a number of "false positives," or authorized users identified as intruders. On the other hand, an attempt to limit false positives by a tight interpretation of intruder behavior will lead to an increase in false negatives, or intruders not identified as intruders. Thus, there is an element of compromise and art in the practice of intrusion detection.

3(Diagram)+
7(Explanation)



[Figure: Profiles of Behavior of Intruders and Authorized Users]

There are two approaches to intrusion detection:

1. **Statistical anomaly detection:** Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.
 - a) **Threshold detection:** This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.
 - b) **Profile based:** A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.
2. **Rule-based detection:** Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.
 - a) **Anomaly detection:** Rules are developed to detect deviation from previous usage patterns.
 - b) **Penetration identification:** An expert system approach that searches for suspicious behavior.

Statistical approaches attempt to define normal, or expected, behavior, whereas rulebased approaches attempt to define proper behavior.

In terms of the types of attackers listed earlier, statistical anomaly detection is effective against masqueraders, who are unlikely to mimic the behavior patterns of the accounts they appropriate. On the other hand, such techniques may be unable to deal with misfeasors. For such attacks, rule-based approaches may be able to recognize events and sequences that, in context, reveal penetration. In practice, a system may exhibit a combination of both approaches to be effective against a broad range of attacks.

7 What is the need of dual signature in SET? Describe with block diagram how they are constructed.

DUAL SIGNATURE:

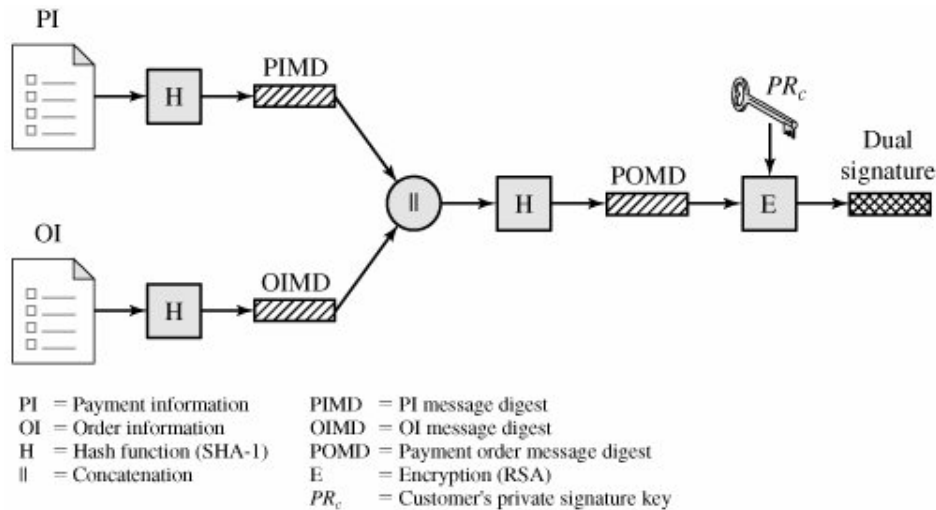
- The purpose of the dual signature is to link two messages that are intended for two different recipients. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank.
- The merchant does not need to know the customer's credit card number, and the bank does not need to know the details of the customer's order.

10

C06 L4

5(Diagram)+
5(Explanation)

- Privacy has to be maintained by keeping these two items separate. However, the two items must be linked in a way that can be used to resolve disputes if necessary. The link is needed so that the customer can prove that this payment is intended for this order and not for some other goods or service.
- Suppose the customers send the merchant two messages: a signed OI and a signed PI, and the merchant passes the PI on to the bank. If the merchant can capture another OI from this customer, the merchant could claim that this OI goes with the PI rather than the original OI. Dual signature could able to prevent this.



[Figure: Construction of Dual Signature]

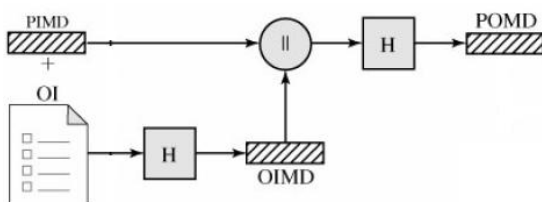
- The customer takes the hash (using SHA-1) of the PI and the hash of the OI. These two hashes are then concatenated and the hash of the result is taken. Finally, the customer encrypts the final hash with his or her private signature key, creating the dual signature. The operation can be summarized as $DS = E(PR_c, [H(H(PI) || H(OI))])$

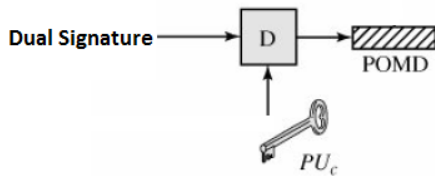
Where

DS is the Dual Signature

PR_c is the customer's private signature key

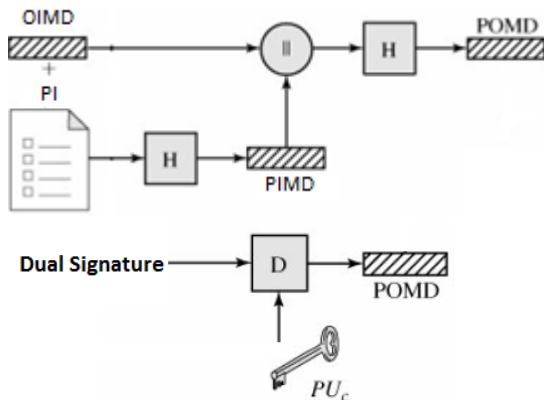
- Merchant has these following informations
 - a) dual signature (DS)
 - b) the OI
 - c) the message digest for the PI (PIMD)
 - d) public key of the customer
 then merchant can compute these two quantities $H(PIMD || H(OI))$ and $D(PUC, DS)$





where PU_c is the customer's public signature key. If these two quantities are equal, then the merchant has verified the signature.

- Similarly if the bank has the following information
 - a) dual signature (DS)
 - b) the PI
 - c) the message digest for the OI (OIMD)
 - d) public key of the customer
 then bank can compute these two quantities $H(H[OI] || OIMD)$ and $D(PU_c, DS)$



if these two quantities are equal, then the bank has verified the signature.

In summary

- 1) The merchant has received OI and verified the signature.
- 2) The bank has received PI and verified the signature.
- 3) The customer has linked the OI and PI and can prove the linkage.

For example, suppose the merchant wishes to substitute another OI in this transaction, to its advantage. It would then have to find another OI whose hash matches the existing OIMD. With SHA-1, this is deemed not to be feasible. Thus, the merchant cannot link another OI with this PI.