Internal Assessment Test 3 – Mar 2018- SCHEME OF EVALUATION

Sub:	Cryptography,Network Security & Cyber law			Code:	15CS61
Date:	21 / 05 / 2018	Duration: 90 mins	Max Marks: 50 Sem: VI	Branch:	ISE

Note: Answer any 5 questions
Total marks: 50

Question #		Description	Marks Distribution		Max Marks
1	a)	Illustrate the types of IPSec protocols with diagram.	5M	5M	10 M
	b)	Compare and contrast tunnel and transport mode in IPSec.	5M	5M	
2	a)	Explain in brief about biometrics and error measures.	5M 5M	5M 5M	10M
3	a)	Illustrate the phases of Internet Key Exchange protocol.	10M	10M	10 M
4	a)	Discuss cyber regulations appellate tribunal.	7M	7M	10 M
	b)	Quote the penalties and adjudication specified by cyber law.	3M	3M	

5	a)	List the offences specified in the cyber law	10M	10M	10 M
6	a)	Infer attribution, acknowledgement and dispatch of electronic records	7M	7M	10M
	b)	Discuss the duties of subscribers specified by cyber law.	3M	3M	
7	a)	Enumerate secure electronic records and secure digital signatures.	10M	10M	10M

Answers

1.a Illustrate the types of IPSec protocols with diagram.

Authentication Header

The Security Authentication Header (AH) is derived partially from previous IETF standards work for authentication of the Simple Network Management Protocol (SNMP) version 2. Authentication Header (AH) is a member of the IPsec protocol suite. AH ensures connectionless integrity by using a hash function and a secret shared key in the AH algorithm. AH also guarantees the data origin by authenticating IP packets. Optionally a sequence number can protect the IP sec packet's contents against replay attacks, using the sliding window technique and discarding old packets.

- In IPv4, AH prevents option-insertion attacks. In IPv6, AH protects both against header insertion attacks and option insertion attacks.
- In IPv4, the AH protects the IP payload and all header fields of an IP datagram except for mutable fields (i.e. those that might be altered in transit), and also IP options such as the IP Security Option (RFC 1108). Mutable (and therefore unauthenticated) IPv4 header fields are DSCP/ToS, ECN, Flags, Fragment Offset, TTL and Header Checksum.
- In IPv6, the AH protects most of the IPv6 base header, AH itself, non-mutable extension headers after the AH, and the IP payload. Protection for the IPv6 header excludes the mutable fields: DSCP, ECN, Flow Label, and Hop Limit.

AH operates directly on top of IP, using IP protocol number 51.

The following AH packet diagram shows how an AH packet is constructed and interpreted:

Authentication Header format																																
Offsets	**Octet$_{16}$**	**0**								**1**								**2**								**3**						
Octet$_{16}$	**Bit$_{10}$**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
0	**0**	Next Header								Payload Len									Reserved														
4	**32**	Security Parameters Index (SPI)																															
8	**64**	Sequence Number																															
C	**96**	Integrity Check Value (ICV)																															
…	**…**	…																															

Next Header (8 bits)
: Type of the next header, indicating what upper-layer protocol was protected. The value is taken from the list of IP protocol numbers.

Payload Len (8 bits)
: The length of this Authentication Header in 4-octet units, minus 2. For example, an AH value of 4 equals 3×(32-bit fixed-length AH fields) + 3×(32-bit ICV fields) − 2 and thus an AH value of 4 means 24 octets. Although the size is measured in 4-octet units, the length of this header needs to be a multiple of 8 octets if carried in an IPv6 packet. This restriction does not apply to an Authentication Header carried in an IPv4 packet.

Reserved (16 bits)
: Reserved for future use (all zeroes until then).

Security Parameters Index (32 bits)
: Arbitrary value which is used (together with the destination IP address) to identify the security association of the receiving party.

Sequence Number (32 bits)
: A monotonic strictly increasing sequence number (incremented by 1 for every packet sent) to prevent replay attacks. When replay detection is enabled, sequence numbers are never reused, because a new security association must be renegotiated before an attempt to increment the sequence number beyond its maximum value.

Integrity Check Value (multiple of 32 bits)
: Variable length check value. It may contain padding to align the field to an 8-octet boundary for IPv6, or a 4-octet boundary for IPv4.

Encapsulating Security Payload

The IP Encapsulating Security Payload (ESP) was researched at the Naval Research Laboratory starting in 1992 as part of a DARPA-sponsored research project, and was openly published by IETF SIPP[20] Working Group drafted in December 1993 as a security extension for SIPP. This ESP was originally derived from the US Department of Defense SP3D protocol, rather than being derived from the ISO Network-Layer Security Protocol (NLSP). The SP3D protocol specification was published by NIST in the late 1980s, but designed by the Secure Data Network System project of the US Department of Defense. Encapsulating Security Payload (ESP) is a member of the IPsec protocol suite. It provides origin authenticity through source authentication, data integrity through hash functions and confidentiality through encryption protection for IP packets. ESP also supports encryption-only and authentication-only configurations, but using encryption without authentication is strongly discouraged because it is insecure.

Unlike Authentication Header (AH), ESP in transport mode does not provide integrity and authentication for the entire IP packet. However, in Tunnel Mode, where the entire original IP packet is encapsulated with a new packet header added, ESP protection is afforded to the whole inner IP packet (including the inner header) while the outer header (including any outer IPv4 options or IPv6 extension headers) remains unprotected. ESP operates directly on top of IP, using IP protocol number 50.

The following ESP packet diagram shows how an ESP packet is constructed and interpreted:

Encapsulating Security Payload format																															
Offsets	**Octet$_{16}$**	**0**								**1**								**2**								**3**					
Octet$_{16}$	**Bit$_{10}$**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
0	**0**	Security Parameters Index (SPI)																													
4	**32**	Sequence Number																													
8	**64**	Payload data																													
…	**…**																														
…	**…**																														
…	**…**	Padding (0-255 octets)																													
…	**…**	Pad Length																									Next Header				
…	**…**	Integrity Check Value (ICV)																													
…	**…**	…																													

Security Parameters Index (32 bits)
: Arbitrary value used (together with the destination IP address) to identify the security association of the receiving party.

Sequence Number (32 bits)
: A monotonically increasing sequence number (incremented by 1 for every packet sent) to protect against replay attacks. There is a separate counter kept for every security association.

Payload data (variable)
: The protected contents of the original IP packet, including any data used to protect the contents (e.g. an Initialisation Vector for the cryptographic algorithm). The type of content that was protected is indicated by the Next Header field.

Padding (0-255 octets)
: Padding for encryption, to extend the payload data to a size that fits the encryption's cipher block size, and to align the next field.

Pad Length (8 bits)
: Size of the padding (in octets).

Next Header (8 bits)
: Type of the next header. The value is taken from the list of IP protocol numbers.

Integrity Check Value (multiple of 32 bits)
: Variable length check value. It may contain padding to align the field to an 8-octet boundary for IPv6, or a 4-octet boundary for IPv4.

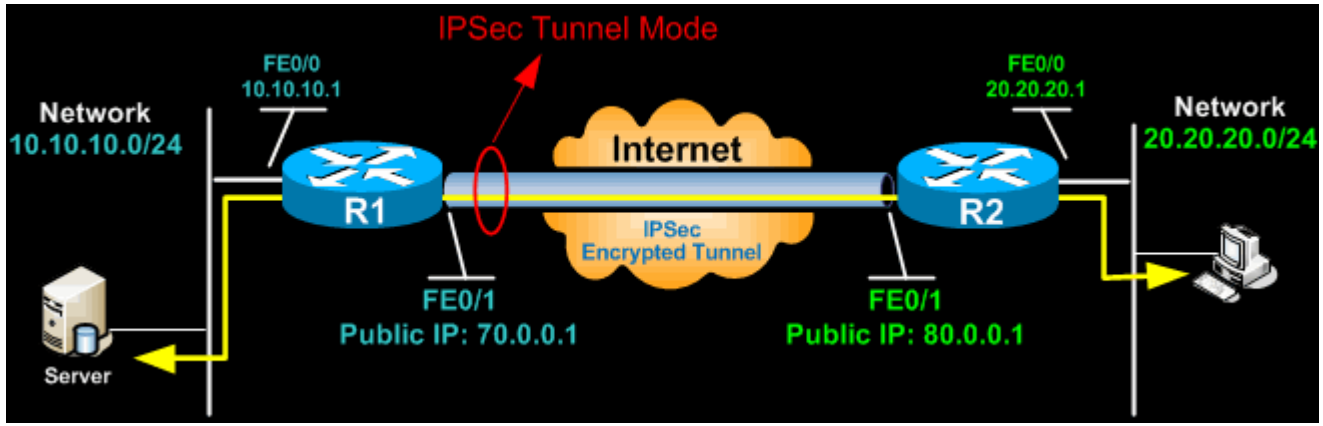
1.b. Compare and contrast tunnel and transport mode in IPSec.

IPSec Tunnel Mode

IPSec tunnel mode is the **default mode**. With tunnel mode, the entire original IP packet is protected by IPSec. This means IPSec wraps the original packet, encrypts it, adds a new IP header and sends it to the other side of the VPN tunnel (IPSec peer).

Tunnel mode is most commonly used between gateways (Cisco routers or ASA firewalls), or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.

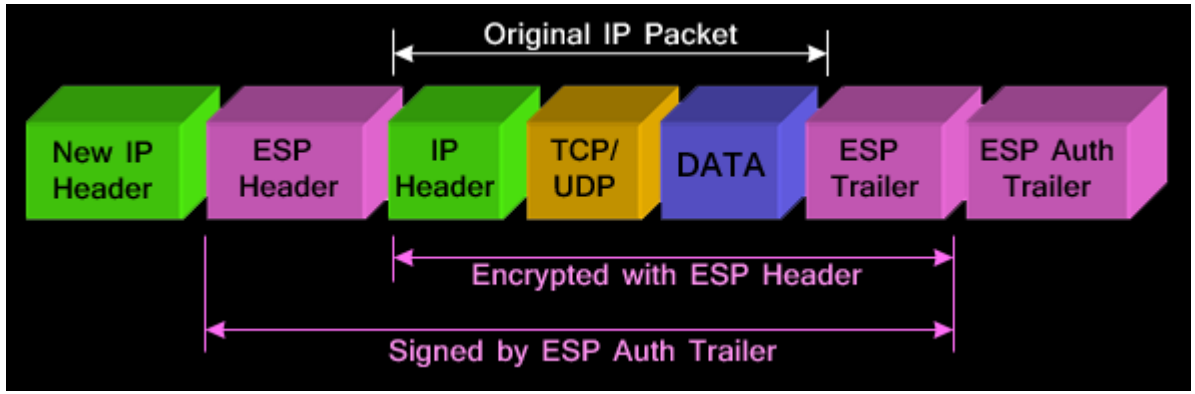
Tunnel mode is used to encrypt traffic between secure IPSec Gateways, for example two Cisco routers connected over the Internet via IPSec VPN. Configuration and setup of this topology is extensively covered in our Site-to-Site IPSec VPN article. In this example, each router acts as an IPSec Gateway for their LAN, providing secure connectivity to the remote network:



Another example of tunnel mode is an IPSec tunnel between a Cisco VPN Client and an IPSec Gateway (e.g ASA5510 or PIX Firewall). The client connects to the IPSec Gateway. Traffic from the client is encrypted, encapsulated inside a new IP packet and sent to the other end. Once decrypted by the firewall appliance, the client's original IP packet is sent to the local network.

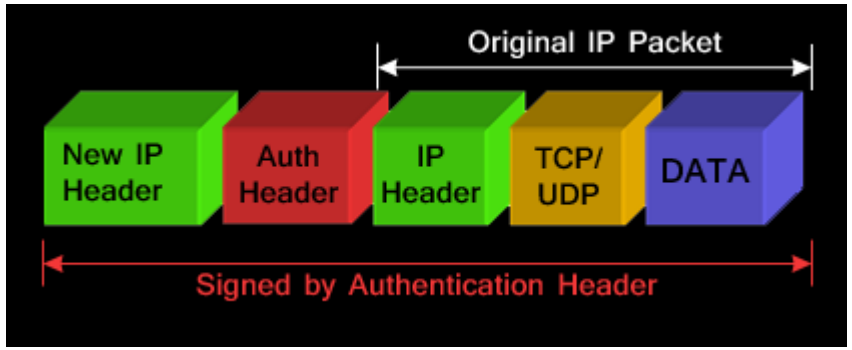
In tunnel mode, an IPSec header (**AH** or **ESP header**) is inserted between the IP header and the upper layer protocol. Between AH and ESP, ESP is most commonly used in IPSec VPN Tunnel configuration.

The packet diagram below illustrates **IPSec Tunnel mode** with **ESP header**:



ESP is identified in the **New IP header** with an IP **protocol ID** of 50.

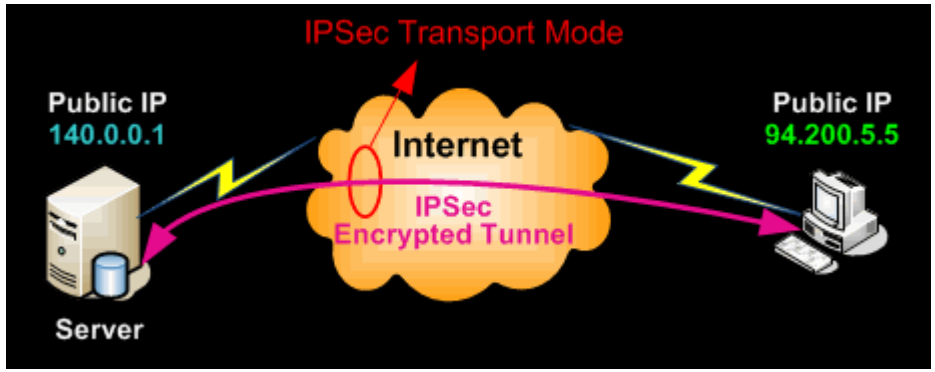
The packet diagram below illustrates **IPSec Tunnel mode** with **AH header**:



The AH can be applied alone or together with the ESP, when IPSec is in tunnel mode. AH's job is to protect the entire packet. The AH does not protect all of the fields in the New IP Header because some change in transit, and the sender cannot predict how they might change. The AH protects everything that does not change in transit. AH is identified in the **New IP header** with an IP **protocol ID** of **51.**

IPSec Transport Mode

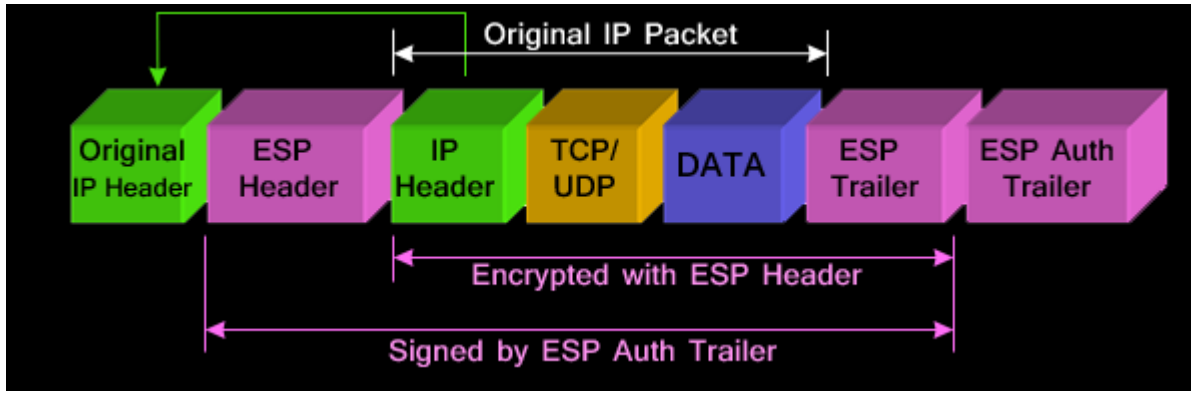
IPSec Transport mode is used for end-to-end communications, for example, for communication between a client and a server or between a workstation and a gateway (if the gateway is being treated as a host). A good example would be an encrypted Telnet or Remote Desktop session from a workstation to a server.



Transport mode provides the protection of our data, also known as IP Payload, and consists of TCP/UDP header + Data, through an AH or ESP header. The payload is encapsulated by the IPSec headers and trailers. The original IP headers remain intact, except that the IP protocol field is changed to ESP (50) or AH (51), and the original protocol value is saved in the IPsec trailer to be restored when the packet is decrypted.

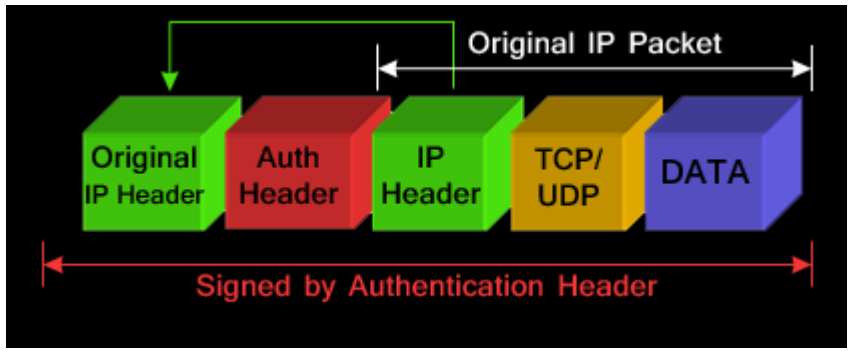
IPSec transport mode is usually used when another tunneling protocol (like GRE) is used to first encapsulate the IP data packet, then IPSec is used to protect the GRE tunnel packets. IPSec protects the GRE tunnel traffic in transport mode.

The packet diagram below illustrates **IPSec Transport mode** with **ESP header**:



Notice that the original IP Header is **moved** to the front. Placing the sender's IP header at the front (with minor changes to the protocol ID), proves that transport mode does not provide protection or encryption to the original IP header and ESP is identified in the **New IP header** with an IP **protocol ID** of **50**.

The packet diagram below illustrates **IPSec Transport mode** with **AH header**:



The AH can be applied alone or together with the ESP when IPSec is in transport mode. AH's job is to **protect** the entire packet, however, IPSec in transport mode does not create a new IP header in front of the packet but places a copy of the original with some minor changes to the protocol ID therefore not providing essential protection to the details contained in the IP header (Source IP, destination IP etc). AH is identified in the **New IP header** with an IP **protocol ID** of **51.**

2.a Explain in brief about biometrics and error measures.

Biometrics(5)

Iis the technical term for body measurements and calculations. It refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

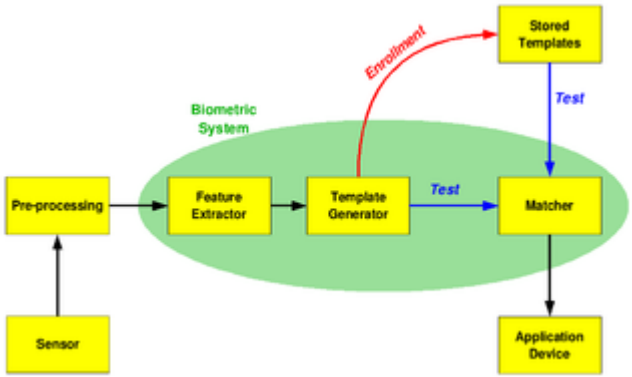
More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain et al. (1999) identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication.

- Universality means that every person using a system should possess the trait.
- Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.
- Permanence relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm.
- Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.
- Performance relates to the accuracy, speed, and robustness of technology used.

- Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.
- Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute.

Proper biometric use is very application dependent. Certain biometrics will be better than others based on the required levels of convenience and security.[8] No single biometric will meet all the requirements of every possible application.



The block diagram illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person. In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".

Second, in identification mode the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

The first time an individual uses a biometric system is called enrollment. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block

(sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the filesize and to protect the identity of the enrollee.

During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements. In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence. Selection of a biometric based on user requirements considers sensor and device availability, computational time and reliability, cost, sensor size and power consumption.

Error Measures (5)

- False match rate (FMR, also called FAR = False Accept Rate): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs that are incorrectly accepted. In case of similarity scale, if the person is an imposter in reality, but the matching score is higher than the threshold, then he is treated as genuine. This increases the FMR, which thus also depends upon the threshold value.[9]
- False non-match rate (FNMR, also called FRR = False Reject Rate): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs that are incorrectly rejected.
- Receiver operating characteristic or relative operating characteristic (ROC): The ROC plot is a visual characterization of the trade-off between the FMR and the FNMR. In general, the matching algorithm performs a decision based on a threshold that determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts. Conversely, a higher threshold will reduce the FMR but increase the FNMR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviation scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).
- Equal error rate or crossover error rate (EER or CER): the rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate.
- Failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

- Failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
- Template capacity: the maximum number of sets of data that can be stored in the system.

3. a. Illustrate the phases of Internet Key Exchange protocol.

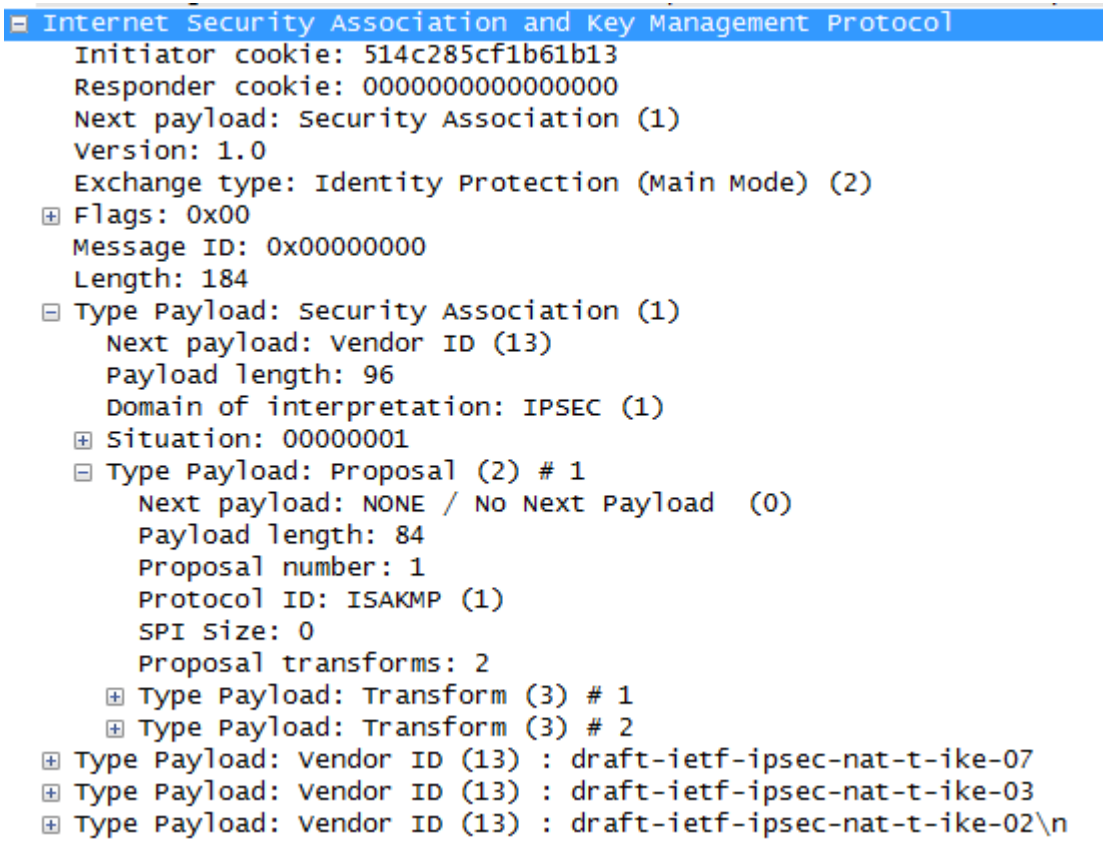
IKE Phase 1

IKE Phase 1 works in one of two modes, main mode or aggressive mode now of course both of these modes operate differently and we will cover both of these modes.

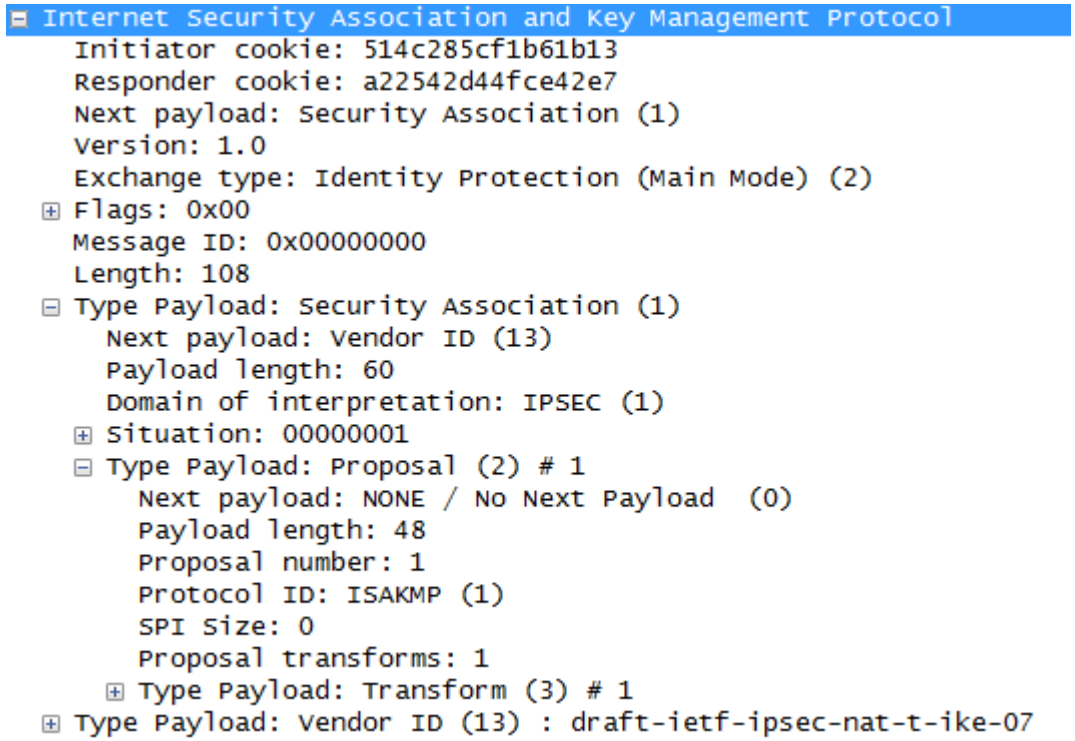
Main Mode:

IKE Phase 1 operating in main mode works with both parties exchanging a total of 6 packets, that's right 6 packets is all it takes to complete phase 1.

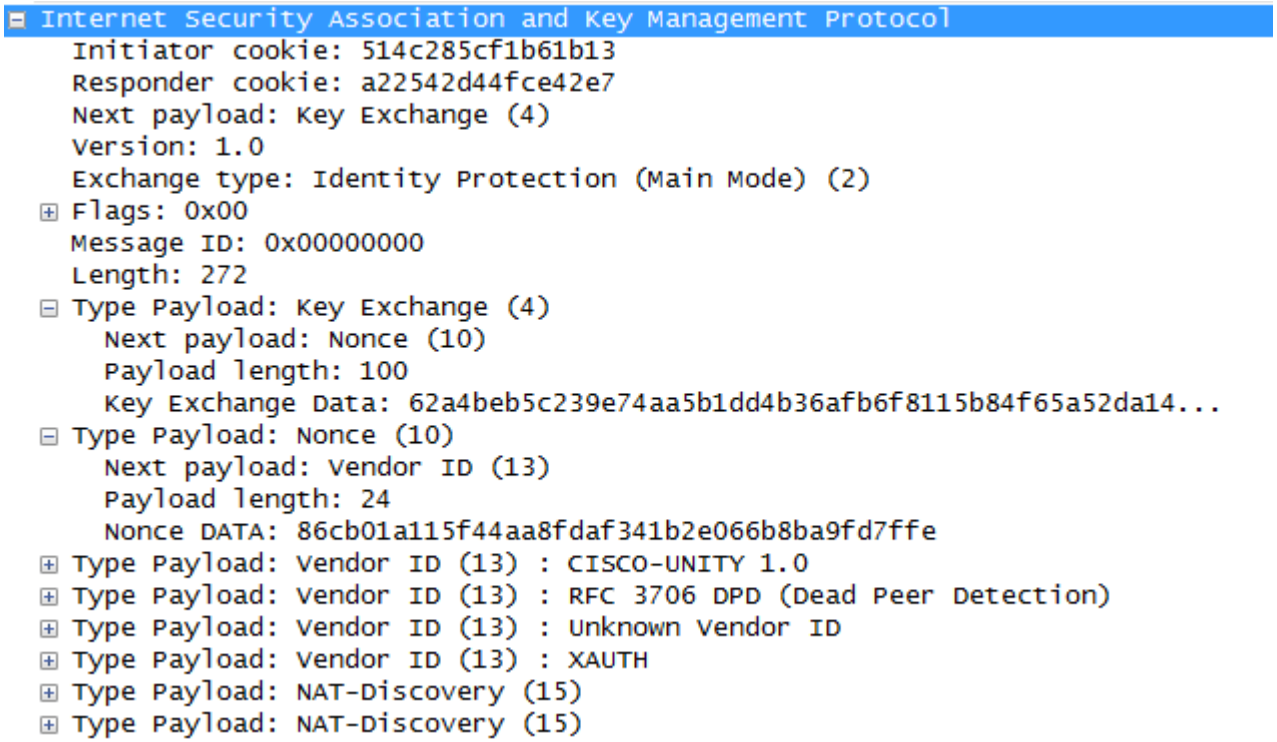
1. The first packet is sent from the initiator of the IPSec tunnel to its remote endpoint, this packet contains the ISAKMP policy
2. The second packet is sent from the remote endpoint back to the initiator, this packet will be the exact same information matching the ISAKMP policy sent by the initiator.
3. The third packet is sent from the initiator to the remote endpoint, this packet contains the Key Exchange payload and the Nonce payload, the purpose of this packet is generate the information for the DH secret key
4. This fourth packet as you would expect comes from the remote endpoint back to initiator and contains the remote endpoints Key Exchange and Nonce payload.
5. The fifth packet is from the initiator back to the remote endpoint with identity and hash payloads, the identity payload has the device's IP Address in, and the hash payload is a combination of keys (including a PSK, if PSK authentication is used)
6. The sixth packet from the remote endpoint to the initiator contains the corresponding hash payloads to verify the exchange.



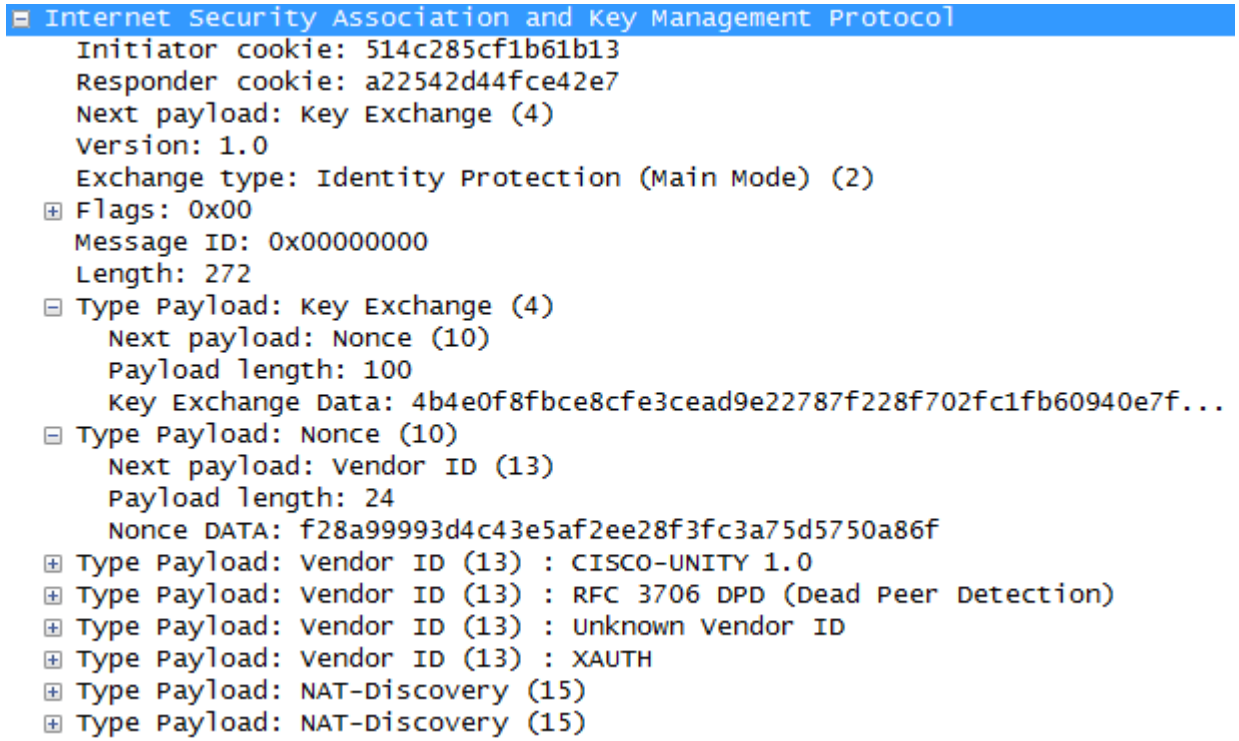
First packet in the IKE Phase 1



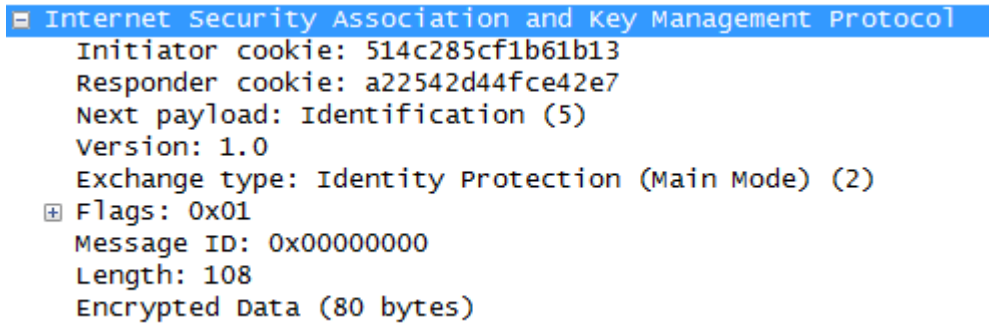
Second packet of the IKE Phase 1 process



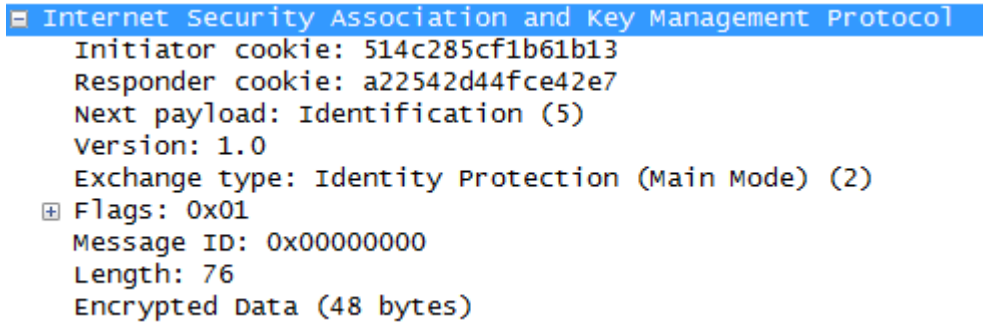
Third packet in IKE Phase 1



Fourth packet in the IKE Phase 1 process



Fifth packet in the IKE Phase 1 process



Sixth and final packet in IKE Phase 1

Aggressive Mode:

IKE Phase 1 operating in aggressive mode only exchanges 3 packets compared to the 6 packets used in main mode. One downside in aggressive is the fact it not as secure as main mode.

1. The first packet from the initiator contains enough information for the remote endpoint to generate its DH secret, so this one packet is equivalent to the first four packets in main mode.
2. The second packet from the remote endpoint back to the initiator contains its DH secret
3. The third packet from the initiator includes identity and hash payloads. After the remote endpoint receives this packet it simply calculates its hash payload and verifies it matches, if it matches then phase one is established.

IKE Phase 2

Now let's look at IKE Phase 2, IKE Phase 2 occurs after phase 1 and is also known as *quick mode* and this process is only 3 packets.

- Perfect Forward Secrecy PFS, if PFS is configured on both endpoints the will generate a new DH key for phase 2/quick mode.

1. Contained in this first packet from the initiator to the remote device are some of the hashes/keys negotiated from phase 1, along with some IPSec parameters IE: Encapsulation (ESP or AH), HMAC, DH-group, and the mode (tunnel or transport)
2. The second packet contains the remote endpoint's response with matching IPSec parameters.
3. The last packet is sent to the remote device to verify the other device is still there and is an active peer.

That last packet concludes the forming an IPSec tunnel and the phase 1/2 process.

- Note: These 3 quick mode packets are encrypted

```
⊟ Internet Security Association and Key Management Protocol
    Initiator cookie: 514c285cf1b61b13
    Responder cookie: a22542d44fce42e7
    Next payload: Hash (8)
    Version: 1.0
    Exchange type: Quick Mode (32)
  ⊞ Flags: 0x01
    Message ID: 0x6c9365ba
    Length: 172
    Encrypted Data (144 bytes)
```

Quick Mode packets with encrypted payload.

5	6.248468	22.22.22.2	11.11.11.2	ISAKMP	226 Identity Protection (Main Mode)
6	6.251858	11.11.11.2	22.22.22.2	ISAKMP	150 Identity Protection (Main Mode)
7	6.254565	22.22.22.2	11.11.11.2	ISAKMP	314 Identity Protection (Main Mode)
8	6.296367	11.11.11.2	22.22.22.2	ISAKMP	314 Identity Protection (Main Mode)
9	6.335913	22.22.22.2	11.11.11.2	ISAKMP	150 Identity Protection (Main Mode)
10	6.339106	11.11.11.2	22.22.22.2	ISAKMP	118 Identity Protection (Main Mode)
11	6.342839	22.22.22.2	11.11.11.2	ISAKMP	214 Quick Mode
12	6.347098	11.11.11.2	22.22.22.2	ISAKMP	214 Quick Mode
13	6.350326	22.22.22.2	11.11.11.2	ISAKMP	102 Quick Mode

4. A. Discuss cyber regulations appellate tribunal.

The Cyber Regulations Appellate Tribunal

48. Establishment of Cyber Appellate Tribunal.

- The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.
- The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

49. Composition of Cyber Appellate Tribunal.

A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Residing Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.

50. Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal.

A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he -

- is, or has been. or is qualified to be, a Judge of a High Court, or
- is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

51. Term of office

The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

52. Salary, allowances and other terms and conditions of service of Presiding Officer.

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of. the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed:

Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

53. Filling up of vacancies.

If, for reason other than temporary absence, any vacancy occurs in the office n the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of. the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed:

Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

54. Resignation and removal.

The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

Provided that the said Presiding Officer shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.

55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.

No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

56. Staff of the Cyber Appellate Tribunal.

- The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit
- The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.
- The salaries, allowances and other conditions of service of the officers and employees or' the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

4.b. Quote the penalties and adjudication specified by cyber law.

PENALTIES AND ADJUDICATION

43. Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network -

- accesses or secures access to such computer, computer system or computer network.

The Gazette of India Extraordinary

- downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium.
- i ntroduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.
- damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network.
- disrupts or causes disruption of any computer, computer system or computer network
- denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means.
- provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder.
- charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation : For the purposes of this section-

- "computer contaminant" means any set of computer instructions that are designed-
  - to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network, or
  - by any means to usurp the normal operation of the computer, computer system, or computer network.
- "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network.
- "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, daia or instruction is executed or some other event takes place in that computer resource.
- "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

44. Penalty for failure to furnish information return, etc.

If any person who is required under this Act or any rules or regulations made thereunder to-

- furnish any document, return or report to the Controller or ?he Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure.

- file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues.

The Gazette of India Extraordinary

- maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

5.a List the offences specified in the cyber law.

PENALTIES AND ADJUDICATION

43. Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network -

- accesses or secures access to such computer, computer system or computer network.

The Gazette of India Extraordinary

- downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium.
- i ntroduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.
- damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network.
- disrupts or causes disruption of any computer, computer system or computer network
- denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means.
- provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder.
- charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation : For the purposes of this section-

- "computer contaminant" means any set of computer instructions that are designed-
    - to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network, or
    - by any means to usurp the normal operation of the computer, computer system, or computer network.
- "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network.
- "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, daia or instruction is executed or some other event takes place in that computer resource.
- "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

44. Penalty for failure to furnish information return, etc.

If any person who is required under this Act or any rules or regulations made thereunder to-

- furnish any document, return or report to the Controller or ?he Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure.
- file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues.

The Gazette of India Extraordinary

- maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

6.a Infer attribution, acknowledgement and dispatch of electronic records.

Attribution, Acknolwedgment and Despatch of Electronic Records

11.Attribution of electronic records.

An electronic record shall be attributed to the originator -

- if it was sent by the originator himself.
- by a person who had the authority to act on behalf of the originator in respect of that electronic record, or
- by an information system programmed by or on behalf of the originator to operate automatically.

12. Acknowledgment of receipt.

- Where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by -
    - any communication by the addressee, automated or otherwise, or
    - any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.
- Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.
- Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

13. Time and place of despatch and receipt of electronic record.

- Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.
- Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely :-
    - if the addressee has designated a computer resource for the purpose of receiving electronic records -
        - receipt occurs at the time when the electronic, record enters the designated computer resource, or
        - if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee.
    - if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.
- Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.
- The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

- For the purposes of this section -
- if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business.
- if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business.
- "usual place of residence", in relation to a body corporate, means the place where it is registered.

6.b. Discuss the duties of subscribers specified by cyber law.

DUTIES OF SUBSCRIBERS

40. Generating key pair.

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

41. Acceptance of Digital Signature Certificate.

- A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate-
    - to one or more persons.
    - in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.
- By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that-
- the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same.
- all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true.
- all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

42. Control of private key.

- Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.
- If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by .the regulations.

Explanation.- For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

7.a. Enumerate secure electronic records and secure digital signatures.

Secure Electronic Records and Secure Digital Signatures

14. Secure electronic record.

Where any security procedure has been applied to an electronic record at a specific point of time. then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

15. Secure digital signature.

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was-

- unique to the subscriber affixing it.
- capable of identifying such subscriber.
- created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated.

then such digital signature shall be deemed to be a secure digital signature.

16. Security procedure.

The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including-

- the nature of the transaction.
- the level of sophistication of the parties with reference to their technological capacity.
- the volume of similar transactions engaged in by other parties.
- the availability of alternatives offered to but rejected by any party.
- the cost of alternative procedures, and
- the procedures in general use for similar types of transactions or communications.