DEPARTMENT OF INFORMATION TECHNOLOGY

U20IT703 /CRYPTOGRAPHY AND NETWORK SECURITY

Unit – 1

Part-A

1.What are the two basic functions used in the encryption algorithm? Nov./dec-14

All the encryption algorithms are based on the two general principles:

Substitution : in which each element in the plain text is mapped into another element.

Transposition : in which each elements in the plain text are rearranged. The fundamental requirement is that no information be lost.

2.What is the difference between an unconditionally secured cipher and a computationally secured cipher?May-10

An encryption scheme is unconditionally secure if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. An encryption scheme is said to be computationally secure if:

1. The cost of breaking the cipher exceeds the value of the encrypted information
2. The time required to break the cipher exceeds the useful lifetime of the information.

3.Why is not practical to use an arbitrary reversible substitution cipher? May : 10

If a small block size, such as n=4, is used , then the system is equivalent to a classical substitution cipher. For small n, such systems are vulnerable to a statistical order of n .. 2^n makes the system impractical . an arbitrary reversible cipher for a large block size is not practical , however, from an implementation and performance point of view. Here the mapping itself is the key.

4. Differentiate passive attack from active attack with example? May :11

Si . no	Passive attack	Active attack
1	Passive attack are in the nature of eavesdropping on, or monitoring of , transmission.	Active attack involves some modification of the data stream or the creation of false stream.
2	Types: release of message content and traffic analysis.	Types: masquerade, reply, modification of message and denial of service.
3	Very difficult to detect.	Easy to detect.
4	The emphasis in dealing with the passive attack is on prevention rather than detection.	It is quite difficult to prevent active attacks absolutely
5	It does not affect the system	It affect the system

5. What is the use of Fermat's theorem? May-11

Fermat's theorem sometimes is helpful for quickly finding a solution to some exponentiations and multiplicative inverses when the modulus is a prime.

6. Give the types of attack? Dec-11

Attack are of two types: passive attack and active attack.

7. List out the problems of one time pad? Dec-11

Problem with one time pad is that of making large quantities of random keys . it also makes the problem of key distribution and protection.

8. Define : Finite field? May-12

Finite field is a field that contains finite number of elements . the finite fields are classified by size, there is exactly one finite field up to isomorphism of size p^k for each prime p and positive integer k.

9. What do you mean by differential cryptanalysis? May-12

Differential cryptanalysis is a method for breaking certain classes of cryptosystems. Differential

cryptanalysis is efficient when the cryptanalyst can choose plaintext and obtain ciphrtext.

10. Define factoring ? may 12

Factoring is the process of finding the factors.

11. What is the difference between a monoalphabetic cipher and polyalphabetic cipher? Dec-12

In mnoalphabetic cipher single cipher alphabet is used per message . But in polyalphabetic cipher there are multiple ciphertext letters for each plaintext leter, one for each uique letter of keyword.

12. What is avalanche effect? Dec-12

Avalanche effect is that a small change in either the plaintext or the key should produce a significant change in the cipher text.

13. Convert the given text "anna university" into cipher text using rail fence technique. may-13

Plaintext = anna university.

Ciphertext = AAIRT NUVSY NNEIA.

14. Define steganography ? May-13

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.

15. Find GCD (21,300) using Euclid's algorithm. May-13

GCD(21,300)

300=14*21+6

21=3*6+3

6=2*3+0

Therefore GCD =3.

16. Why modular arithmetic has been used in cryptography? Dec-13

Application of modular are given to block ciphers in cryptography . modular arithmetic directly underpins public key system such as RSA and Diffie-Hell man as well as providing finite fields which underlie elliptic curves and is usd in a variety of symmetric key algorithms including AES. IDEA and RC4.

17. List out the classical encryption techniques. Dec-15

Classical encryption techniques are :Caesar cipher, monoalphabetic cipher , playfair cipher, hill cipher , polyalphabetic situation, one time pad and feistel cipher.

18.Define symmetric encryption ?dec-15

In symmetric encryption, sender and receiver use same key for encryption and decryption.

19. What is discrete logarithm problem? May-14

Discrete Logarithm Problem(DLP) is easy to perform and hard to reserve. The strength of one way function is based on one time needed to reserve it .

Let be a cyclic finite group and g G be a generator of G. the DLP in G is following:

Given an element h G , find the smallest positive integer x such that

H=[x]g (additive group)

h= g^x (multiplicative group)

x is denoted as: x=D log(h).

20.Find 11^7 mod 13 ?may-15

Step 1 : 11^2 =121 =4(mod 13)

Step 2: 11^4= (11)=42= (mod 13)

Step 3 : 11^7 = 11*4*3=132=2(mod 13)

Unit – 2

Part-A

1.What is primitive root? May-15

A primitive root of a prime p is an integer g such that g(mod p) has multiplicative order

2. State the difference between conventional encryption and public-key encryption. Dec-11

Conventional encryption : same algorithm and same key is used for encryption and decryption. Sender and receiver must share the algorithm and key. Key must be kept secret.

Public-key encryption : one algorithm is used for encryption and decryption with pair of keys. The sender and receiver must each have one of the matched pair of keys. One of two keys must be kept secret.

3. Mention the application of public key cryptography? Dec-15

1. Encryption /Decryption.
2. Digital signature.
3. Key exchange.

4. What is key distribution center? Dec-13

A key distribution center is responsible for distributing keys to pairs of users such as hosts, processes, applications. Each users must share a unique key with the key distribution center for purposes of key distribution.

5. State few applications of RC4 algorithm. May-15

RC4 is used in SSL/TLS. It is also used in WEP, the IEEE 802.11 wireless networking security standard . it can be found in a number of other applications including email encryption products.

6.What is AES cipher?dec-15

Advanced Encryption Standard(AES) is a symmetric key block cipher. AES is a non Feistal cipher that encrypts and decrypts a data block of 128bits. The key size can be 128,192 or 256 bits. It depends on number of rounds . the number of rounds:10rounds for 128 bits , 12round for 192 bits , and 14 rounds for 256 bits.

7. Point out the types of cryptanalytic attack?dec-14

Cipher text only,
Known plain text,
Chosen plaintext,
Chosen cipher text.

8. Is it possible to use the DES algorithm to generate message authentication code. Justify? dec-14

Yes. It can be any blocks a MAC. Data authentication Algorithm(DAA) is a widely used MAC based on DES-CBC. Encrypt message using DES n CBC mode and send just the final block as the MAC.

9. List the difference between stream and block cipher? Dec-14

s.no	***Stream cipher***	***Block cipher***
1	Stream cipher operates on smaller units of plain text	Block cipher operates on larger blocks of data
2	Faster than block cipher	Slower than stream cipher
3	Require less code	Requires more code
4	Only one time of key used	Reuse of key is possible
5	Ex-one time pad	Ex-DES

10. State whether symmetric and asymmetric cryptopraphic algorithm need key exchange? May-14

Most encryption algorithm require source of random data. Random numbers are necessary not only for generating cryptopraphic keys but are also needed in steps of cryptographic algorithms or protocols.

11.List the use of RC4?dec-13

RC4 has become part of some commonly used encryption protocols and standard such as WEP, WPA,, TLS ,Kerberos and SASL mechanism digest MD5.

12. What are the modes of DES? Dec-13

1. Electronic Code Book (ECB)
2. Cipher Block Chaining(CBC)
3. Cipher Feedback (CFB)
4 . Output feed(OFB)
5 . Counter (CTR)

13. What is weak collision resistance? What is the use of it? May-13

Weak collision-resistance: given an x and h(x), it is infeasible t find x' such that h(x)=h(x'). this implies that given h(x), it is infeasible to find any x' such that h(x)=h(x').

14. What is the disadvantages with ECB mode of operation ?may-13

Disadvantages:

a) synchronization error is unrecoverable
b) Not suitable for lengthy messages.

15. Name any two methods for testing prime numbers? May-11

Testing prime numbers methods are divisibility algorithm and probabilistic algorithms.

16. What are the different modes of operation in DES? MAY-11

1. Electronic Codebook Book (ECB) : Message is broken into independent blocks of 64 bits.
2. Cipher Block chaining(CBC) : Message is broken in independent blocks of 64 bits, but next input depends on previous output.
3. Cipher Feedback (CFB) : the message is XORed with the feedback of encrypting the previous blocks.
4. Output Feedback: the feedback is independent of the message.

17. What is the difference between statistical randomness and unpredictability? May-10

In application such as reciprocal authentication and session key generation is the requirement is not so much that the sequence of numbers be statistically random but that the successive numbers of the sequence are unpredictable. With true random sequence each number s statistically independent of other numbers in the sequence and therefore unpredictable.

18. List out the ingredients of public key encryption scheme? Dec-09

a) Plaintext b)Encryption algorithm
c) Public key d) Private key
e) Cipher key f) Decryption key

19. What was the final set of criteria used by NIST to evaluate candidate AES ciphers? May-10

a) General security, b) Software implementations
c) Restricted space environment, d) Hardware implementations
e) Attack on implementations, f) Encryption Vs. Decryption
g) Key agility, h) other versatility and flexibility
i) Potential for instruction- level parallelism.

20. What are the disadvantages of double DES? (Nov/Dec-12)

The following are the disadvantages of double DES

1. Reduction to a single stage.
2. Meet in the middle attacks.
3. Double DES is less secure than triple DES.
4. Double DES is within brute force attack.

Unit – 3

Part-A

1.What are the two types of certificates? May-10

Two types of certificates are:

a) Forward certificates
b) Reverse certificates

2.What is birthday attack? May-11

A birthday attack is a name used to refer to class of brute-force attacks. It gets its name from the surprising result that the probability that two or more people in a group of 23 share the same birthday is greater than ½: such a result is called result paradox.

3. What do you mean by one-way property in hash function? May-11

For any given value h, it is computationally infeasible to find x such that H(x)=h.

4. What is digital signature? May-15

Digital signature is an authentication mechanism that enables the creator of a message to attach a code that act as a signature.

5.What is one way property? Dec-12

A function that maps an arbitrary length message to a fixed length message digest is a one way hash function if it is one way function.

6.What are the two approaches of the digital signature? Dec-12

Two approaches of digital signature are RSA approach and DSS approaches.

7. write any two differences between MD4 and secure hash algorithm. Dec-13

s.no	MD4	SHA
1	Pad message so its length is 448 mod 512	Pad message so its length is a multiple of 512 bits
2	Initialize the 4-word (128-bit) buffer (A,B, C,D)	Initialize 5-bit (160 bit)buffer(A,B,C,D)
3	Process the message in 16-word chunks using 3 rounds of 16 bit operation each on chunk and buffer	Process the message in 16-word chunks using 4 rounds of 20 bit operations.

8. List the authentication requirements? May-14

1. Disclosure 2. Traffic analysis
3. Masquerade 4. Sequence modification
5. Content modification 6. Timing modifications
7. Source repudiation 8. Destination repudiation

9. Name the authentication protocols? DEC-15

Kerberos is an authentication protocol. It provides a way to authenticate clients to services to each other through a trusted third party.

10. List four requirements that were defined for Kerberos? Dec-15

Security
Reliability
Transparency
Scalability

11. List any four password selection strategies? Dec-15

User education
Computer generated password
Reactive password checking
Proactive password checking

12.What are the security services provided by digital signature? Dec-14

Security services provided by digital signature are message authentications, message integrity of a message. Message authentication is an mechanism or service used to verify the integrity of a messages. Integrity ensures that information is not changed or altered in transit. When a message is sent the receiver can prove that the alleged sender in fact sent the message.

13. What is message authentication?

It is a procedure that verifies whether the received message comes from assigned source has not been altered. It uses message authentication codes, hash algorithms to authenticate the message.

14. Differentiate MAC and hash function?

MAC:

In message authentication code, the secret key shared by sender and receiver. The MAC is appended to the message at the source at the time which the message is assumed or known to be correct.

Hash function:

The hash value s appended to the message at the source at time when the message is assumed or known to be correct. The hash function itself not considered to be secret .

15 .Write any three hash algorithms?

MD5 (Message Digest Version 5) algorithm.

SHA_1(Secure Hash Algorithm).

RIPEMD_160algrithm.

16. What is weak collision resistance? What is the use of it? (M/J-13)

For any given block x, It is computationally infeasible to find Y X with H(Y) H(X). It guarantees than an alternative message hashing to the same value as a given message cannot found. This prevents forgery when as encrypted hash code is used.

17. What is meant by EIGamal cryptosystem? (A/M-11)

The ElGamal system is a public-key cryptosystem based on the discrete logarithm problem. It consists of both encryption and signature algorithms. The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol.

18.. List out the requirements of Kerberos. (A/M -11)

The requirements of Kerberos are as follows:

(1) Secure (2) Reliable (3) Transparent (4) Scalable

19.What is the difference between a message authentication code and a one-way hash function? (N/D-09)

A hash function, by itself, does not provide message authentication. A secret key must be used in some fashion with the hash function to produce authentication. A MAC, by definition, uses a secret key to calculate a code used for authentication.

20.What is a hash function? (N/D-09)

A hash function H is a transformation that takes a variable-size input m and returns a fixed-size string, which is called the hash value h (that is, h = H(m)). Hash functions with just this property have a variety of general computational uses, but when employed in cryptography the hash functions are usually chosen to have some additional properties.

Unit – 4

Part-A questions

1. What is a worm?(dec 2013)

A worm is a program designed to copy itself and send copies from a computer to other computer across the network.

2. What is Trojan horse?(may 2011)

A Trojan horse is a program that appears to be useful but that actually does damage.

3. What is logic bomb?(may 2013)

A logic bomb is a software embedded in some legitimate programs and is set to explode under certain conditions.

4. What are the major issues derived by porras about the design of a distributed intrusion detecting system?(may 2010)

porras point out following major issues:

a) System may need to deal with different audit record formats

b) One or more nodes in the network will serve as collision and analysis points for the data from the system on the networks.

c) Either centralized or decentralized architecture can be used

5. What are the three main components involved in the distributed intrusion defect system? (may 2010)

a) Host agent schedule: An audit collection module operating as a background process on a monitored system

b) Lan monitor agent module: same as host agent module except that it analysis LAN traffic and transports.

6 .Define intruder. Name three classes of intruders.(may 2011)

An intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system. classes of intruders: masquerader, misfeasor, clandestine user.

7. What is honey pot?(may 2011)

A system placed there just so it will be attacked so attackers waste time ,and so the attackers will be analyzed

8. Write down the role of security standards?(may 2011)

Standards allow products from multiple vendors to communicate, giving the purchaser more flexibility in equipment selection in use

9. Define intrusion(may 2012)

Intrusion is an illegal act of entering, seizing or taking possession of another property

10 .Write down the system security standards .(may 2012)

security standards development and publications re done by internet architecture board, internet engineering task force, and internet engineering steering group

11. Give few examples for worms. (dec 2012)

Morris worm and Myndoom

12. Mention the two levels of hackers. (may2013)

Two levels of hackers are criminal hackers, disgruntled employees, ideological hackers and underemployed adult hackers etc.,

13. What are the effects of malicious software? Write any two.(dec2013)

The effects of malicious viruses on a computer system include occupation of disk space. Tantacle 2 VIRUS WILL CHANGE ICONS ON A COMPUTER SCREEN.

14. Differentiate spyware and virus?(may 2014)

S.no	Spyware	virus

1	Spyware is specific unwanted software that collects user information without appropriate notice and consent	A virus is a specific software that can be spread from computer to computer usually by e-mail
2	Spyware tries to stick to the computer	Virus spread throughout the system i.e. one computer to other

15. What are zombies? (may2014)

Zombies are computer connected to internet that has been compromised by a hacker, computer virus or Trojan horse and can be used to perform malicious tasks under remote directions

16 .List out the requirements of Kerberos.(may 2011)

The four requirements for Kerberos are; secure, reliable, transparent, and scalable.

17 .Define malicious software? (dec2011)

Malicious software is any software that gives partial to full control of your computer to do whatever the malware creator wants .Malware can be a virus ,worm, Trojan, adware ,spyware ,root kit etc.,

18. What are the certificates revoked in X.509?(may 2015)

User ‘s private key is compromised.

User is not certified by CA

CA’s certificate is compromised

19. Differentiate macro virus and boot virus?(dec 2014)

A macro virus is a platform independent virtually all of the macro viruses infect MS word documents. macro viruses take advantages of a feature found in word and other office applications such as Microsoft excel, namely the macro. Boot sector virus infects a master boot record or boot record and spreads when a system is booted from the disk containing virus

20. Lit out the difference between virus and worms.(dec 2015)

VIRUS: a computer virus is a program that loaded on your computer without your knowledge and runs without your permission .A virus is designed to reproduce itself through legitimate process in computer programs and operating systems therefore , a virus requires a host in order to replicate .viruses are often cable of mutating or changing while they are replicating themselves.

Unit – 5

Part-A

1. What is MIME and S/MIME?(May 2011)

Multipurpose Internet Mail Extensions(MIME) is supplementary protocol that allows non-ASCII data to be sent through e-mail. Secure/Multipurpose Internet Mail Extension extends the protocols of MIME by adding digital signatures and encryption to them. S/MIME is not restricted to mail; it can be used with any transport mechanism that transports MIME data, such as HTTP.

2. Define TLS.(May 2012)

Transport Layer Security (TLS) is a protocol that encrypts and delivers mail securely.TLS encryption the use of a digital certificate, which contains identity information about the certificate owner as well as a public key, used for encrypting communications.

3. What do you mean by S/MIME?(May 2012)

S/MIME is a security enhancement to the MIME Internet E-mail format standard, based on technology from RSA Data Security. S/MIME provides the cryptographic security services for electronic messaging applications: authentication, message integrity, non- repudiation of origin, privacy and data security.

4. What are the different types of MIME? (Dec 2012)

MIME types are text, Multipart, Message type, Image type, Video type, Audio type and Application type.

5.What protocols comprises SSL?(Dec 2012)

SSL Record Protocol , SSL Handshake Protocol, SSL Change Cipher Spec etc.

6.List out the services provided by PGP.(May 2013)

Services provided by PGP are digital signature, message encryption, compression, e-mail compatibility and segmentation.

7.Expand and define SPI.(May/Dec 2013)

The Security Parameter Index (SPI) is an identification tag added to the header while using IPSec for tunneling the IP traffic. The tag helps the kernel discern between two traffic streams where different encryption rules and algorithms may be in use.

8. Define SET.(Dec- 13)

Secure Electric Transaction (SET) is an open encryption and security specification designed to protect credit card transactions on internet.

9. What are the applications involved in IP Security?(May 2010)

Application of IP security

a) Provide secure communication across private and public LAN.

b) Secure remote access over the internet.

c) Secure communication to other organization.

10. Mention four SSL protocols.(May 2011)

Four SSL protocols are:

1) Handshaking protocol: Establish communication variables.

2) Change cipher spec protocol: Alert to a change in communication variables.

3) Alert protocol: Messages important to SSL connections.

4) Application encryption protocol: Encrypt / Decrypt application data.

11.List the limitations of SMTP/RFC 822. (Nov/Dec 2016)

1.Transfer a data limited size

2. Gateways don't always between the map properly between EBCDIC and ASCII

3.It cannot diacritical marks.

4. It cannot handle non-text data in x. 400 message

12.Define Botnets. (Nov/Dec 2016)

A Botnet (also known as a zombie army) is a number of internet computers that although their owners are unaware of it, have been set up to forward transmissions to other on the internal.

13. Draw the ESP packet format.(Apr/May 2017)

Security Parameter Index
Sequence number
Payload data(variable)
Paddling (0-255)bytes
Pad length Next header
Authentication Data(variable)

14.Specify the benefits of IPSec. (Apr/May 2017)

It is a virtual private network (VPN) is a virtual operates across the public network but remains private

1. Data integrity 2. Authentication 3. Confidentiality

15.What do you mean by PGP?(Dec 2013)

PGP stands for Pretty Good Privacy. It was developed originally by Phil Zimmerman. However, in its incarnation as open PGP, it has now become an open standard. PGP is open- source. Although PGP can be used for protecting data in long- term storage, it is used primarily for email security.

16. What is optimal asymmetric encryption padding?(May 2014/Dec 2013)

Optimal Asymmetric Encryption Padding(OAEP): OAEP is the main standard padding for RSA public key encryption: a way to format the message before encryption in order to reach a higher security level.

17. What are the protocols used to provide IP Security?(Dec 2014)

Authentication header (AH) protocol and Encapsulating Security Payload (ESP) used to provide IP security.

18. What is tunnel mode in IP security?(May 2015)

Tunnel mode provides protection to entire IP packets. Security fields are added to IP packets and entire packet is new IP packet with a new IP header. Entire new IP packet travels through a tunnel from one point to other over IP network. No routers over the network are able to detect inner IP header. Since original packet is encapsulated by new larger packet having different source and destination address.

19. What are the five principal services provided by PGP? (AU:Dec-15)

Principle services provided by PGP are:

Access control
Connectionless integrity
Data origin authentication
Rejection of packets, confidentially

20.Define SET? (AU:Dec-13)

Secure electric transaction (SET) is an open encryption and security specification designed to protect credit card transaction on internet.

21. Expand and define SPL (May-13)

The security parameter index (SPI) is an identification tag added to the header while using IP security for tunneling the IP traffic .This tag helps the kernel discern between two traffic streams where different encryption rules and algorithm may be in use .