Name:- Prashant Raj

Roll:- 13000116084

~~Paper~~
Subject :- Cryptography and
Network security

Paper Code :- CS 801 D

Stream :- CSE (sec-A)

CA - 4

1 Ans :- Difference between diffusion and confusion are :-

Confusion	Diffusion
i) Utilized to generate vague cyphertexts	i) Utilized to generate obscure, plain, text.
ii) Makes a relation between statistics of the cyphertext and the value of encryption key as complicated as possible.	ii) The statistical relationship between the plain text and ciphertext is made as complicated as possible.
iii) Substitution Algorithm	iii) Transposition Algorithm.
iv) Block cipher only	iv) stream cipher and block cipher.
v) Increased vagueness	v) Increased Redundancy

2. Ans:-

Given $p = 13$, $q = 17$

$n = 13 \times 17 = 221$ and

$\phi = (13-1) \times (17-1) = 12 \times 16 = 192$

$e = 35$ (publickey)

A	B	D	K
1	0	192	-
0	1	35	5
1	-5	17	2
-2	11	1	-

$d = 11$

Hence $n = 221$, $e = 35$, $d = 11$.

4. Ans:- Pretty Good Privacy or PGP is a popular program used to encrypt and decrypt email over the internet as well as authenticate messages with digital signatures and encrypted stored files. PGP uses a variation of the public key system. In this system each user has an encryption key

that is publicly known and a private key that is known only to that user. You encrypt your message you send to someone else using their public key. When they recieve it they decrypt it using their private key. Since encryption of an entire message is time consuming PGP uses a faster encryption algorithm to encrypt the messages and then use the public key to encrypt the shorter key that was used to encrypt the entire messag Both the encrypted message and short key are sent to the reciever who first uses the reciever's private key to decrypt the short key and and then uses tha key to decrypt the message.

5. Ans!- Properties that digital signature should have are !-

i) It must verify the author and date and time of the signature.

ii) It must authenticate the contents at the time of signature.

iii) It must be verifiable by third parties, to resolve disputes.

6. Ans!- Four basic principles related to security of messages are:-

i) Confidentiality :- This is the most obvious idea associated with security of message and Messages are encrypted using algorithms and secret keys which are only known by the sender and reciever. This makes it hard for attackers to decrypt the message

ii) Authentication!- This is the process of identifying yourself to your communication partner.

iii) Integrity!- These are means ~~deployed~~ employed to ensure a reciever gets the message which was intended for them and vice versa. Through integrity, one can ensure no transmission has been altered or transferred message appears as it was when send.

iv) Non-repudiation!- These are the measure put in place ensure the sender agrees to have sent the message, not an impersonator. This is basically a legal liability. If you agree to the message, it means that you are legally obligated. Non-repudation can be compared to a signature on the contract.