INFORMATION SECURITY

Assignment – 1

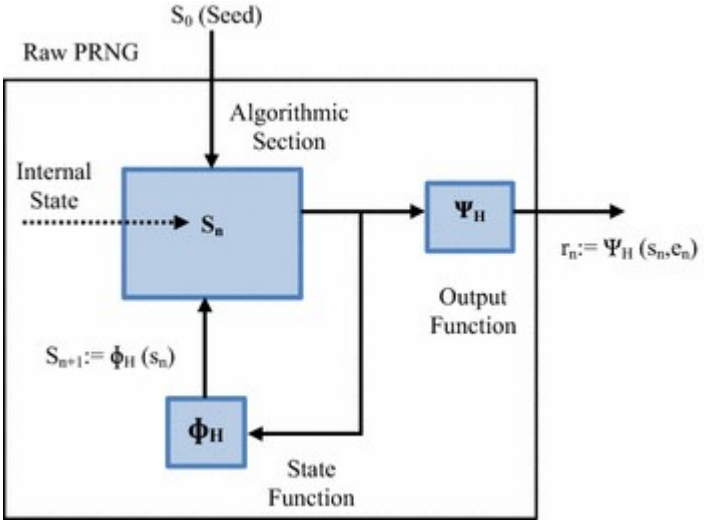
1)

a. List the significance of Pseudo Random Number Generator (PRNG) algorithm in context to information security.

-> It is quite efficient where we require multiple random numbers which should not be repeating and it can be done in short period of time.

-> The seed chosen for PRNG should be such that it can't be predicted at a later stage or it should not be repeating. This is commonly achieved by either using time or date of system or both. This reduces the chances of prediction of numbers.

b. Draw the flow diagram of PRNG algorithm of your choice.



c. How the seed value must be supplied to the PRNG according to you. Justify your answer.

-> The seed chosen for PRNG should be such that it can't be predicted at a later stage or it should not be repeating. This is commonly achieved by either using time or date of system or both. This reduces the chances of prediction of numbers.

2)

a. List the requirements of a PRNG.

The general requirement of secrecy of output of PRNG requires:

-> Randomness

-> Unpredictability

-> Characteristics of the seed

b. Explain Blum Blum Shub Generator with an example.

-> It is basically of form $x_{n+1} = x_n^2 \bmod M$

-> Eg. Let p=11, q=23 and s=3 (where s is the seed). We can expect to get a large cycle length for those small numbers, because ((p-3)/2,(q-3)/2)=2 ((p-3)/2,(q-3)/2)=2. The generator starts to evaluate x_0 by using x_{-1}=s and creates the sequence 9, 81, 236, 36, 31, 202. The following table shows the output (in bits) for the different bit selection methods used to determine the output.

Parity bit	Least significant bit
0 1 1 0 1 0	1 1 0 0 1 0

3)

a. List the properties of stream cipher.

-> Main function used is XOR

-> Key is generated using PRNGs.

b. Explain Stream Cipher structure.

-> In this, each bit of plain text is XORed with the key which is generated randomly which in result gives cipher text, method known as encryption.

-> This cipher text is XORed with same key which again gives the plain text which is method of decryption.

4)

a. Which is the stream cipher practically used in SSL/WEP/WPA?

-> Rivest Cipher 4 is used.

b. Explain the working of the stream cipher mentioned as answer to a. using a diagram.

-> You input a secret key and the text you'd like to protect.

-> The cipher scrambles your text via encryption. The work happens byte by byte rather than in chunks.

-> Your scrambled text heads to the recipient. That person should have a copy of the secret key you used to protect the data.

-> The recipient walks back through these steps to uncover your original text.