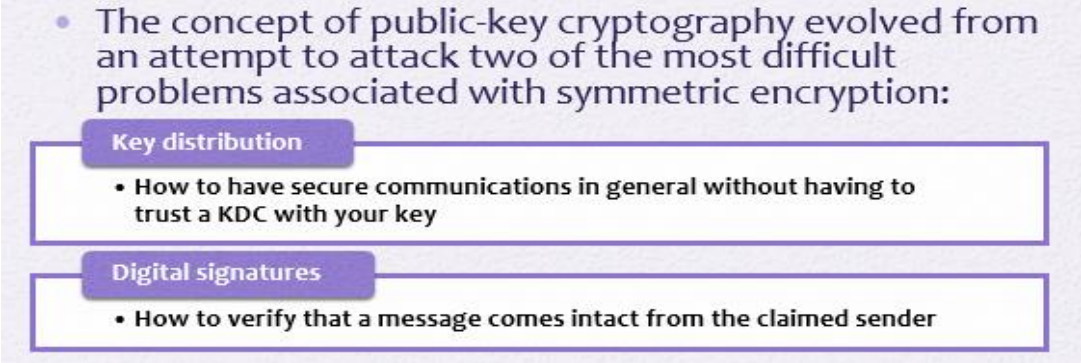
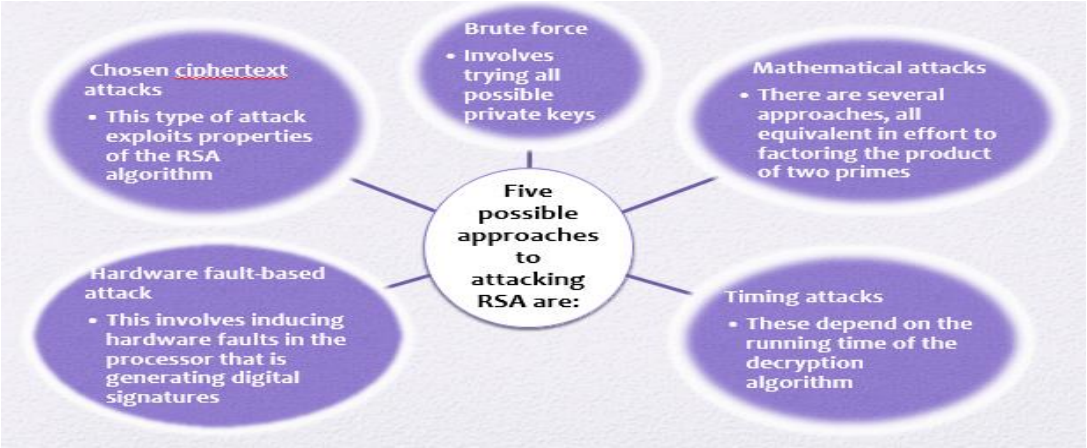
Q1) The concept of Public-Key Cryptography evolved from an attempt to attack most difficult problems associated with symmetric encryption, Describe these problems? Classify categories of PKC? List possible approaches to attacking RSA are:

ANS: Describe these problems



ANS: Classify the categories of PKC:

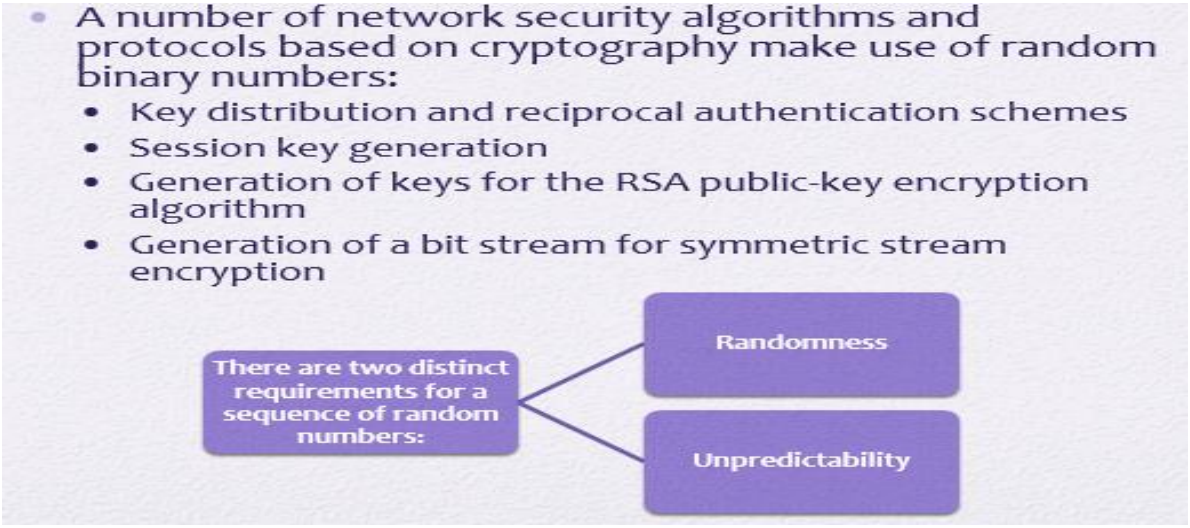
ANS: List possible approaches to attacking RSA:



Q2) Pseudorandom number generators (PRNGs) are used in a variety of cryptographic and security applications.

A. **A number of network security algorithms and protocols based on cryptography make use of random binary numbers, Describe these algorithms and protocol.**
B. **There are distinct requirements for a sequence of random numbers, Describe it?**
C. **Summarizes using Table only the principal differences between PRNGs and TRNGs.**
D. **Describe approaches that use a block cipher to build a PNRG have gained widespread acceptance?**

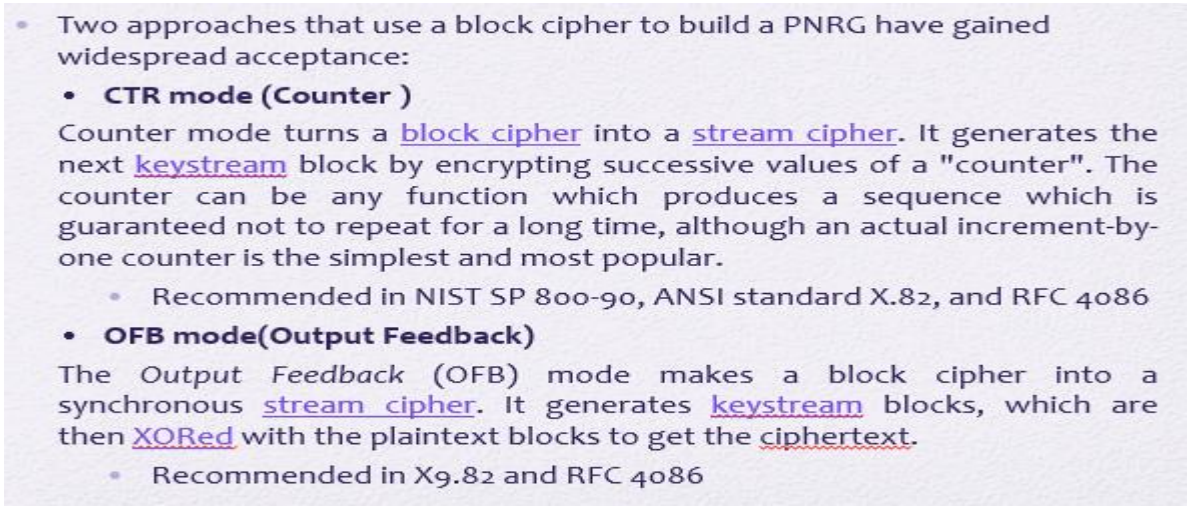
ANS: (A,B)



ANS: (C)

	Pseudorandom Number Generators	True Random Number Generators
Efficiency	Very efficient	Generally inefficient
Determinism	Deterministic	Nondeterministic
Periodicity	Periodic	Aperiodic

ANS: (D)



Q3) Answer the following questions:

1) Decrypt the encrypted message "**GYDPPKLRSMGOVM**" Using PlayFair Algorithm with Keyword "**DARKROOMS**":
2) Differentiate between Cryptanalysis and Brute-Force Attack
3) Describe Steganography? Various other techniques have been used historically; Give examples?

ANS: (1)

Playfair keyword
DARKROOMS

Action
Decrypt

Playfair square

D	A	R	K	O
M	S	B	C	E
F	G	H	I	L
N	P	Q	T	U
V	W	X	Y	Z

Transformed text
IWANTAHOMELAND

ANS: (2)

- **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
- **Brute-force attack:** The attacker tries every possible key on a piece of cipher-text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

ANS: (3)

Steganography: A plaintext message may be hidden in one of two ways. The methods of **steganography** conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.

- **Character marking:** Selected letters of printed or typewritten text are over-written in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.
- **Invisible ink:** A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
- **Pin punctures:** Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.
- **Typewriter correction ribbon:** Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Q4) Answer the following questions:

1) **Using Table only, Describe difficulties in defending against attacks?**
2) **Illustrate using Figure only Information security components?**

ANS: (1)

Reason	Description
Universally connected devices	Attackers from anywhere in the world can send attacks
Increased speed of attacks	Attackers can launch attacks against millions of computers within minutes
Greater sophistication of attacks	Attack tools vary their behavior so the same attack appears differently each time
Availability and simplicity of attack tools	Attacks are no longer limited to highly skilled attackers
Faster detection of vulnerabilities	Attackers can discover security holes in hardware or software more quickly
Delays in patching	Vendors are overwhelmed trying to keep pace by updating their products against attacks
Weak patch distribution	Many software products lack a means to distribute security patches in a timely fashion
Distributed attacks	Attackers use thousands of computers in an attack against a single computer or network
User confusion	Users are required to make difficult security decisions with little or no instruction

Table 1-2 Difficulties in defending against attacks

ANS: (2)

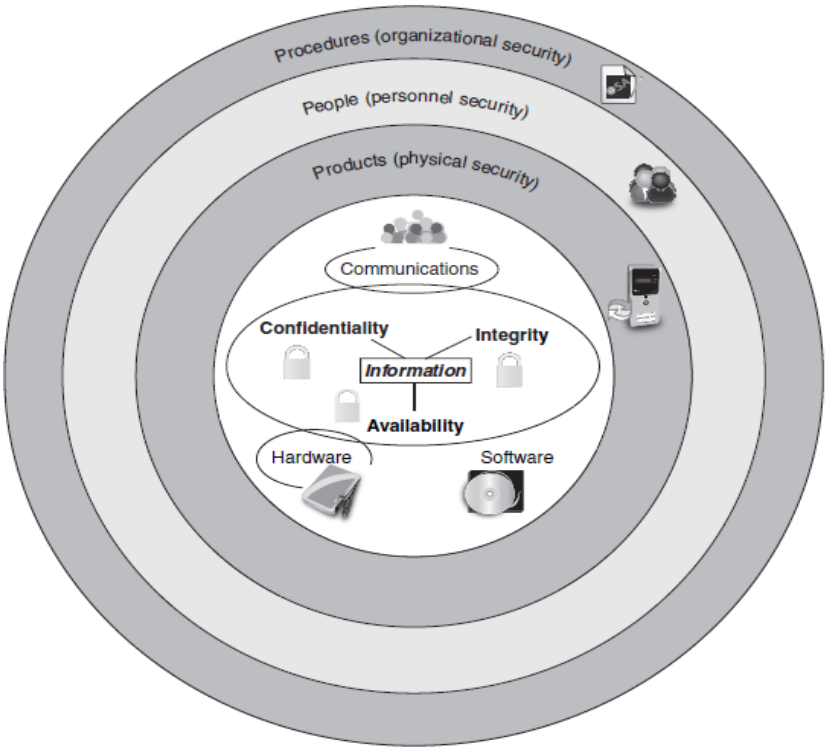


Figure 1-3 Information security components