COVID – 19 (ONLINE EXAMINATION)

DSVV

देव संस्कृति विश्वविद्यालय

शान्तिकुन्ज, हरिद्वार

आन्तरिक मूल्यांकन परीक्षा – INTERNAL EVALUATION TEST

उत्तर-पुस्तिका

परीक्षार्थी अनुक्रमांक (अंकों में) 1824020
Student's Roll No. (in numbers)

परीक्षार्थी अनुक्रमांक (शब्दों में) Sujeet Kum
Student's Roll No. (in words)

कक्षा BCA (6th Sem)
Class

दिनाँक 26/03/21
Date

प्रश्न पत्र संख्या .....
Examination Paper Number

पेपर कोड .....
Paper code

नामांकन संख्या .....
Enrollment Number

विषय Cryptography
Subject

दिन Friday
Day

लघुत्तरीय	योग/Total
A) Short Answer Type	
1 2	
दीर्घ उत्तरीय	
B) Long Answer Type	
1	
कुल योग अंकों में / TOTAL IN DIGITS	
कुल योग शब्दों में/TOTAL IN WORDS	

Sujit Kr
परीक्षार्थी के हस्ताक्षर
Signature of student's

परीक्षक के हस्ताक्षर
Signature of Examiner

Date

Page No.

Short Answer Questions

1. Cryptosystems:

- Cryptosystems are complex combinations of hardware and software that are used to transform plaintext message into a series of unintelligible characters, known as cipher text then back to their original plaintext form.

- The authentiety and integrity of an encrypted message required the use of digital signatures and one-way hashes

The two type of cryptosystem

i) Symmetric:-

- Symmetric Key systems, or Secret Key systems, rely on the same key to encrypt and decrypt ciphet text, so ensuring that the secret key is not compromised is extermely important.

- The length of the keys used by different systems varies.

- Symmetric cryptosystems either encrypt data in a stream, bit by bit or in block form, usually 64 bits at a time.

Teacher's Signature

Shivalik

Asymmetric Cryptosystems

- Asymmetric Key Systems, or public Key System, use both a private and public Key for encrypting and decrypting ciphertext.
- Another important advantage of asymmetric system is that they provide enhanced security in the form of digital signatures and strong Key Managment.
- SHA-1 is a hashing algorithm, ideal for proving message integrity.
- SHA-1 is used in SSL and IPSec.
- Certificates are available for individuals, organizations, servers and software developers.

Perfecty Security.

- The notions of perfect security is also called as unconditional security information-theorotty security.
- The attack moded considered in the definition of perefect security is ciphertext only-attack.
- It is assumed that attacker is computationally unbounded
- Prefect secrecy achieved when.

  a posteriori probilites = a priori probabilities.

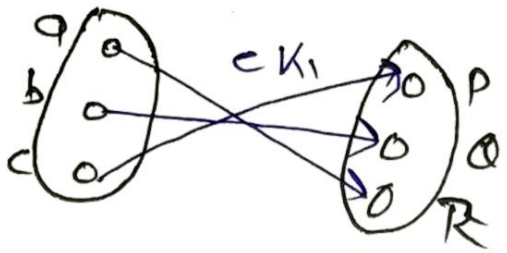
$$Pr[X|H] = Pr[X]$$

  i.e the attack learns nathing from the ciphertext.

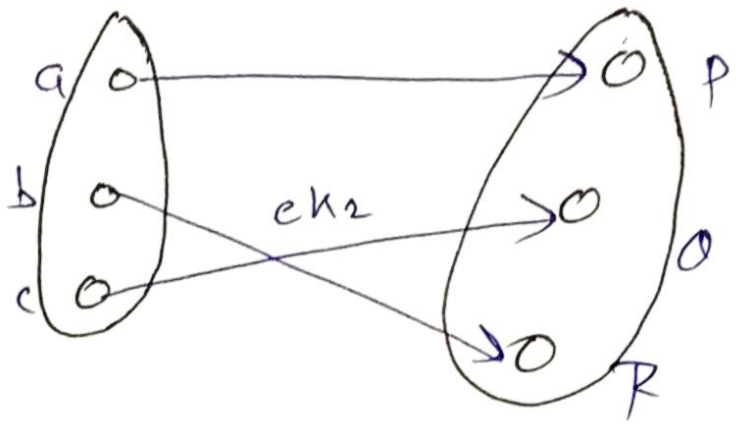
Example

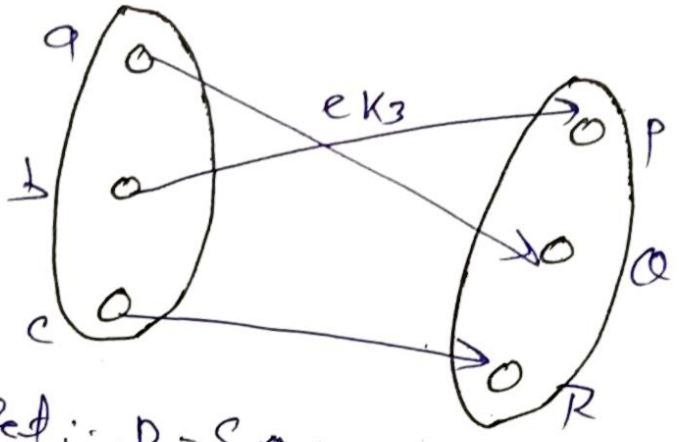
- Find the a posteriori probabilites for the following scheme
- Verify that it is perfectly secret.

Plaintext
$Pr[X=a] = 1/2$
$Pr[X=b] = 1/3$
$Pr[X=K_6] = 1/6$



Keyspace
$Pr[K=K_1]=1/3$
$Pr[K=K_2]=1/3$
$Pr[K=K_3]=1/3$





- Plaintext set :- $P=\{0,1,2,3,\ldots,25\}$
- Ciphertext set :- $C=\{0,1,2,3,\ldots,25\}$
- Keyspace : $K=\{0,1,2,3,\ldots,25\}$
- Encryption Rule : $e_K(x)=(x+K) \bmod 26$,
- Decryption Rule : $d_K(x)=(x-K) \bmod 26$

where $K \in K$ and $x \in P$.

Date

Page No. 5

Long Answer Question

1. OSI Security Architecture:-

- To assess effectively the security needs of organisation and to evaluate and choose various security products and policies, we need some systematic way of defining the requirements for security and characterising the approaches to satisfying those requirements.

- The OSI Security Architecture focuses on three essential parts:-

i Security Attack:- Any action that compromise the security of information owned by a organisation

- Security attacks can be classified into passive attack and active attacks.

- A passive attack attempts to learn or make use of information from a system without affecting system resources.

- An active attack attempts to modify system resources or effect their operations.

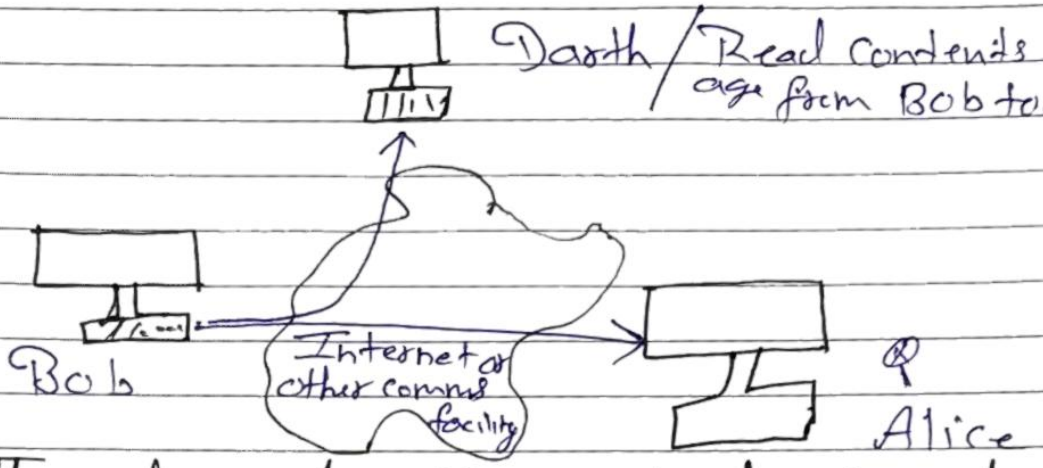
ii) Passive Attack:- The goal of opponent is to obtain information that is being transmitted.

Two types of passive attack are the release of message contents and traffic analysis

Teacher's Signature

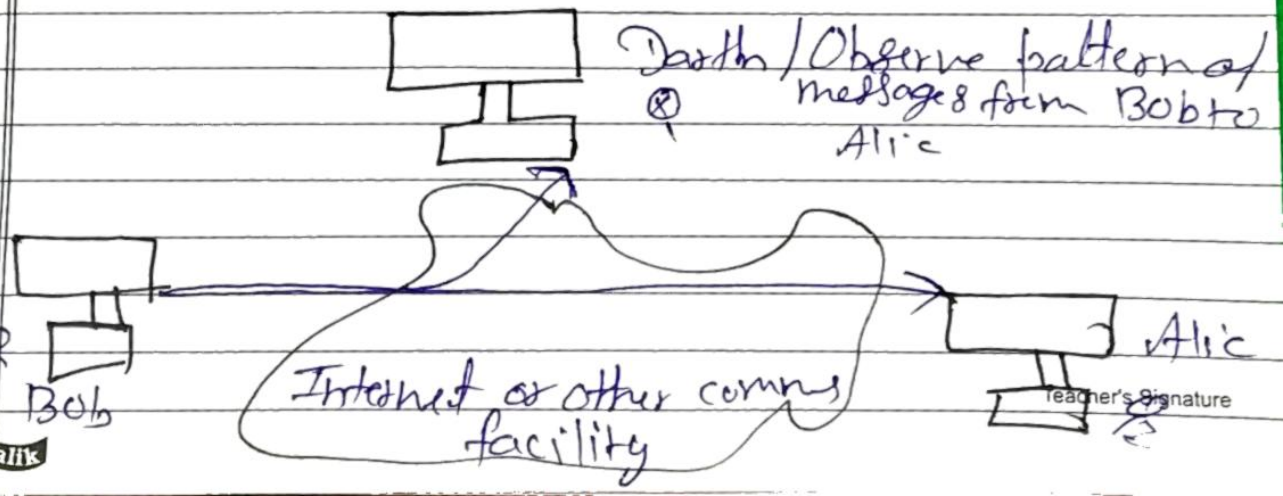
Shivalik

- Release of Message contents



- The release of message contents is quite clear. For example Somebody is watching your secret email, monitoring what information you are sending and receiving.

- Traffic analysis:- The hacker might not see the contents but could determine the location, identify the communication hosts and observe the regular frequency and the length of exchanged message.



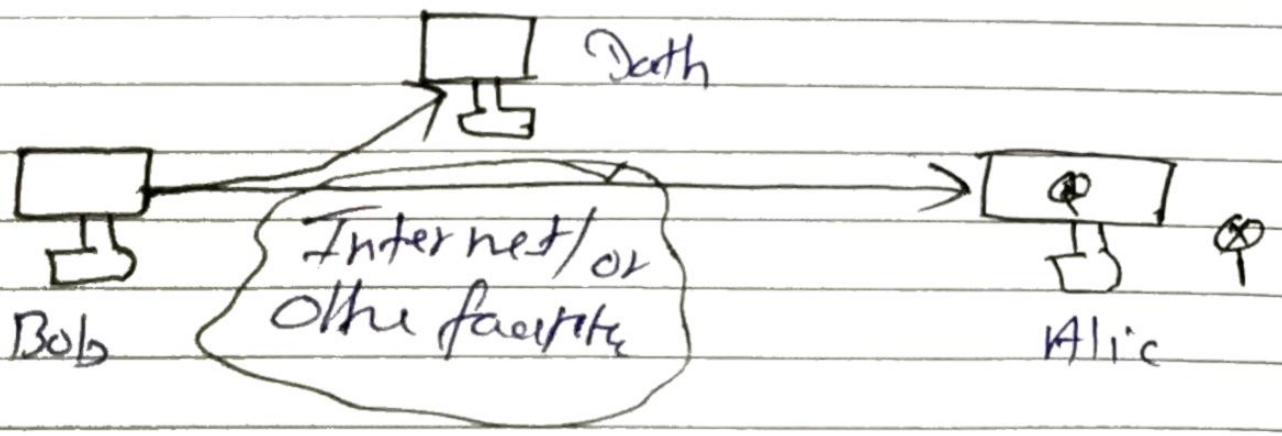
Security mechanism: Any process that is used to detect, prevent or recover from a security attack.

Security Service: Any processing or communication service that enhances the security of data processing systems and the information transformation of an organisation.

Active attack:-

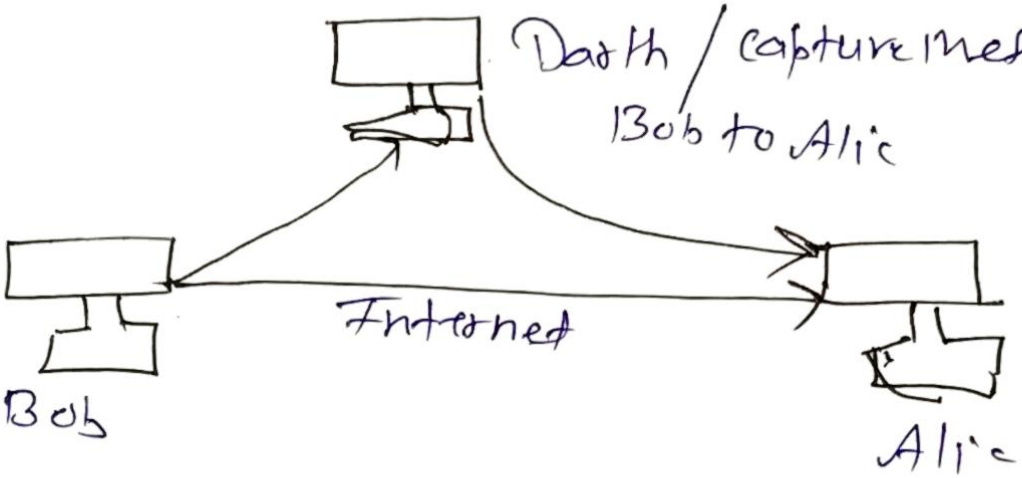
- Active attack involves some modification of data stream and creation of false stream.
- It can be divided into four categories.

i) Masquerade: One entity pretends to be a different entity. For example



Teacher's Signature

ii) Rplay:- refers to the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect



iii) Modifactions of message: means some portion of a legitimate message is altered. for example message mens "I am sujit" is altered to be I am Komal.