



देव संस्कृति विश्वविद्यालय

शान्तिकुण्ड, हरिद्वार

आन्तरिक मूल्यांकन परीक्षा - INTERNAL EVALUATION TEST

उत्तर-पुस्तिका

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

1824020

पेपर कोड
Paper code

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

Eighteen

नामांकन संख्या
Enrollment Number

कक्षा
Class

BCA (6th Sem)

विषय
Subject

Cryptography

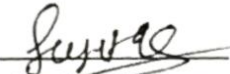
दिनांक
Date

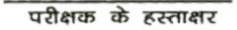
27/02/2021

दिन
Day

Saturday

प्रश्न पत्र संख्या
Examination Paper Number


परीक्षार्थी के हस्ताक्षर
Signature of student's


परीक्षक के हस्ताक्षर
Signature of Examiner

लघु उत्तरीय		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		

Short Answer Question

①

Q1. What do you mean by cryptographic primitive? Describe them briefly.

Ans. A cryptographic primitive is a low-level algorithm used to build cryptographic protocols for a security system.

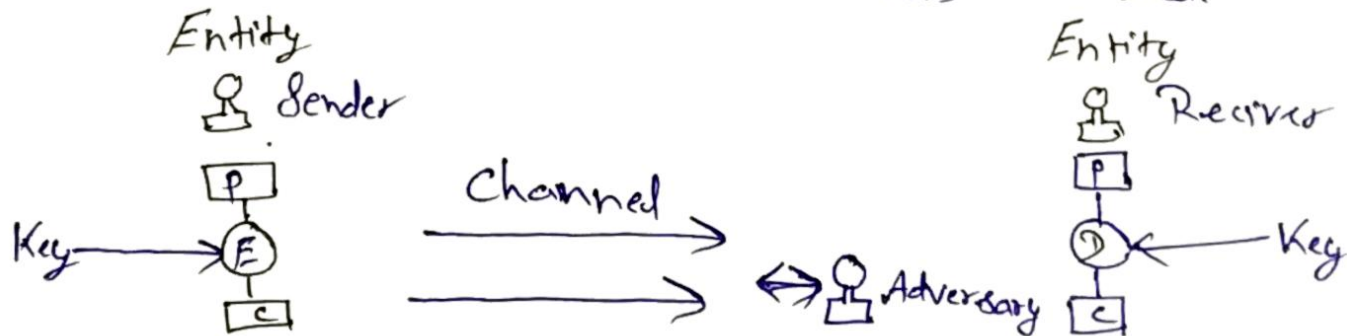
- A security protocol is a set of steps taken in order to achieve a required security goal utilizing appropriate security machines.
- Various type of security protocols are in use, such as authentication protocols, non-repudiation protocols, and key management protocols.
- It's used by cryptographic designer as their most basic building blocks.

• Common cryptographic primitives:

- One-way hash function :- A mathematical function takes a variable-length input string and converts it into a fixed-length binary sequence.

(2)

- Symmetric key cryptography: An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt message.
- Public Key Cryptography: Also known as asymmetric cryptography, a system that uses a pair of keys: a public key and private key.
- Mix-network: A routing protocol that creates hard-to-trace communications.
- Private information retrieval: A protocol that allows a client to retrieve database information without the owner of the database knowing what specific information was retrieved.



Q2.

3

State the applications of cryptography.

- Cryptography was in implementation only for securing purposes.
- Wax seals, hand signatures and few other kind of security methods were generally utilized to make sure of reliability and accuracy of the transmitter.
- Authentication / Digital Signatures:- Authentication is any process through which one proves and verifies certain information.
- Time Stamping:- Time stamping is a technique that can certify that a certain electronic document or communication existed or was delivered at a certain time.
- Electronic money:- The definition of electronic money (also called electronic cash or digital cash) is a term that is still evolving.
- Encryption / Decryption in email:- Email encryption is a method of securing the content of emails from anyone outside of the email conversation, looking to obtain a participant's information.

- Encryption in WhatsApp:- WhatsApp uses the "Signal" protocol for encryption, which uses a combination of asymmetric and symmetric key cryptographic algorithms.
- Encryption in Instagram:- ~~For~~ Your interaction with Instagram is likely end-to-end encrypted communication.
- SIM Card Authentication:- Authentication To decide whether or not the SIM may access the network, the SIM needs to be authenticated.

5

Long Answer Question

Q1. A

The classical algorithms are those invented before computer era until around the 1980's. The list below is roughly ordered by complexity, least complex at the top.

Some type of classical cryptanalysis.

i) Shift cipher:- Caesar cipher:-

- The Caesar cipher can be broken in milliseconds using automated tools. Since there are only 25 possible keys (each possible shift of the alphabet), we just try decrypting the ciphertext using each key and determine the fitness of each decryption.

- This form of solution is known as brute force solution, and is only possible for the very simplest of ciphers

Example

Our ciphertext is following:

AMTJHFOXFWHNUM...

To find out what the original was, we try decrypting it. With each of the 25 possible keys calculating the fitness for each trial decryption.

output THE CAESAR CIPHER

i) Mono alphabets - Simple substitution cipher

ii) Mono alphabets - Simple substitution cipher

- The simple substitution cipher is one of the simple ciphers, simple enough that it can usually be broken with the open and paper in a few minutes.
- On this page we will focus on automatic cryptanalysts of substitution cipher.

Example To begin the algorithm, we generate a random key, e.g.

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

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

(7)

and decipher the ciphertext using this key to get

CHBMSRTPD - - - - -

After many iterations of this approach, the final key that was found was

XZTJWUMOBEPARIQKDLFSCHXGNV

iii) Polycalphabets - Vigenere cipher

- The vigenere cipher was thought to be completely unbreakable for hundreds of years, and indeed, if very long keys are used the vigenere cipher can be unbreakable.
- Cryptanalysis of the vigenere cipher has 2 main steps: identify the period of the cipher (the length of the key) then find the key.

Example

- The vigenere cipher applies different Caesar ciphers to consecutive letters. If the key is "PUB", the first letter is enciphered with a Caesar cipher with key (P is the 16th letter of the alphabet), the second letter with another and the third letter with another.
- As a result if we gather letters 1, 4, 7, 10 --- we should get a sequence of characters.
- The sequence of characters 2, 5, 8, 11 --- and 3, 6, 9, 12 --- will also be enciphered with their own Caesar cipher.