



देव संस्कृति विश्वविद्यालय

शान्तिकुन्ज, हरिद्वार

आन्तरिक मूल्यांकन परीक्षा - INTERNAL EVALUATION TEST

**उत्तर-पुस्तिका**

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

1824014

पेपर कोड  
Paper code

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

Pranav Mishra

नामांकन संख्या  
Enrollment Number

1800000137

कक्षा  
Class

BCA

विषय  
Subject

Cryptography

दिनांक  
Date

27-02-2021

दिन  
Day

Saturday

प्रश्न पत्र संख्या

Examination Paper Number

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		

परीक्षार्थी के हस्ताक्षर  
Signature of student's

Pranav

परीक्षक के हस्ताक्षर  
Signature of Examiner

Ans:-1 Cryptographic Primitive :-

A Cryptographic Primitive is a low-level algorithm used to build Cryptographic Protocols for a security system. It's used by Cryptographic designers as their most basic building blocks. These building blocks are a part of a cryptosystem, which is a suite of cryptographic algorithms needed to implement a particular security service, such as encryption functions or one way hash functions.

- ~~For~~ Creating and testing a primitive to be reliable task a long time and is very hard, so designing a new cryptographic primitive to suite the needs of a new cryptographic system is very rare.
- Cryptographic primitive are similar to programming languages
- It's rare a programmer will invent a new programming language while writing a new program.

→ Common Cryptographic Primitives:-

- 1:- One way hash function
- 2:- Symmetric Key Cryptography
- 3:- Public Key Cryptography
- 4:- Private information retrieval
- 5:- Mix Network.

## Ans:- 2 Application of Cryptography:-

### Authentication/Digital Signatures:-

- Authentication is any process through which one proves and verifies certain information.
- The identity of the sender, the time and date a document was sent or signed.
- A digital signature is a cryptographic means through many of these may be verified.

Time Stamping:- Time stamping is a technique that can verify that a certain electronic document was delivered at a certain time.

Electronic Money:- The definition of electronic money is a term that is still evolving.

- There are both hardware and software implementations.

### Encryption/Decryption in email:-

I will use email in daily life. Email encryption is a method of securing the contents of email.

### Sim Card Authentication:-

Authentication to decide whether or not the sim may access the network. The sim needs to be authenticated. A number is generated by the operator and sent to the mobile devices.



Ans:- Classical Cipher:-

A classical cipher is a type of cipher that was used historically but for the most part, has fallen into disuse. In contrast to modern cryptography algorithms, most classical ciphers can be practically computed and solved by hand.

There are three types: ~~of~~

- Shift cipher
- Mono alphabetic Substitution cipher
- Poly-alphabetic Substitution (Vigenere) cipher

# Shift Cipher:- Plain-text and cipher-text character  $E \in \{a, \dots, z\}$

- Encryption: shift each plain text character by 'k' positions "forward"
- Decryption:- Shift each cipher text character by 'k' positions "backward"
- $k \in \{0, \dots, 25\}$  and randomly selected by the key-generation algorithm
- Mathematical interpretation of the shift cipher:-
  - interpret the set  $\{a, \dots, z\}$  as  $\{0, \dots, 25\}$
  - $k \in \{0, \dots, 25\}$  and  $M = C = \text{set of strings over } \{0, \dots, 25\}$

Examples:- Text:- ATTACK AT ONCE  
 Shift:- 4  
 Cipher:- EXXEGIOEXSRGI

## Cryptanalysis of Shift Cipher:-

- Plaintext:  $m = \{m_1, \dots, m_n\}$
- Ciphertext:  $c_i = \{c_1, \dots, c_n\}$
- Attack model: Ciphertext Only Attack (COA)
  - Information known to attacker
    - Ciphertext
    - Process through which the ciphertext is generated i.e.  $c_i = (m_i + k) \bmod 26$
  - Attack
    - An attacker can try to decrypt  $c$  with all possible  $k$
    - Easy to mount! only 26 candidate keys
- Learning:-
  - Sufficient key space principle:-

## # Mono Alphabetic Substitute Cipher:-

- Map each plaintext character to an arbitrary ciphertext character in a one to one fashion.
  - Key: A secret permutation (determined by the key generation algo)
- Brute-force attack is impractical
  - No. of candidate keys  $= (26!) \approx 2^{88}$

Cryptanalysis of Mono Alphabetic Substitution cipher

- frequency analysis: applicable when plaintext space is a natural language

Ex:- It would include the shift cipher, each letter is shifted based on numeric key 5:-

- Idea! exploit the redundancy present in the underlying natural language.

## # Poly alphabetic Substitution Cipher:-

- A poly alphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
- The Vigenere cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

### Cryptoanalysis:-

- Two stage approach:-

Stage 1:- Determine the length of the unknown key.

— Kasiski method, Index of coincidence method

Step 2:- Try to determine the character  $k_1, k_2, \dots, k_x$

- Independent instances of letter frequency analysis

Ex:- Input: Plaintext: GREEKSFORGREEKS  
Keyword: AYUSH

Output: Ciphertext: GXCZFMZYLEIM