COVID – 19 (ONLINE EXAMINATION)

DSVV

देव संस्कृति विश्वविद्यालय

शान्तिकुन्ज, हरिद्वार

आन्तरिक मूल्यांकन परीक्षा – INTERNAL EVALUATION TEST

उत्तर–पुस्तिका

परीक्षार्थी अनुक्रमांक (अंकों में) 1824096
Student's Roll No. (in numbers)

पेपर कोड .....
Paper code

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

नामांकन संख्या 18000012g
Enrollment Number

कक्षा BCA (VI Semester)
Class

विषय Cryptography
Subject

दिनाँक 27-02-2021
Date

दिन Saturday
Day

प्रश्न पत्र संख्या .....
Examination Paper Number

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

Aniket

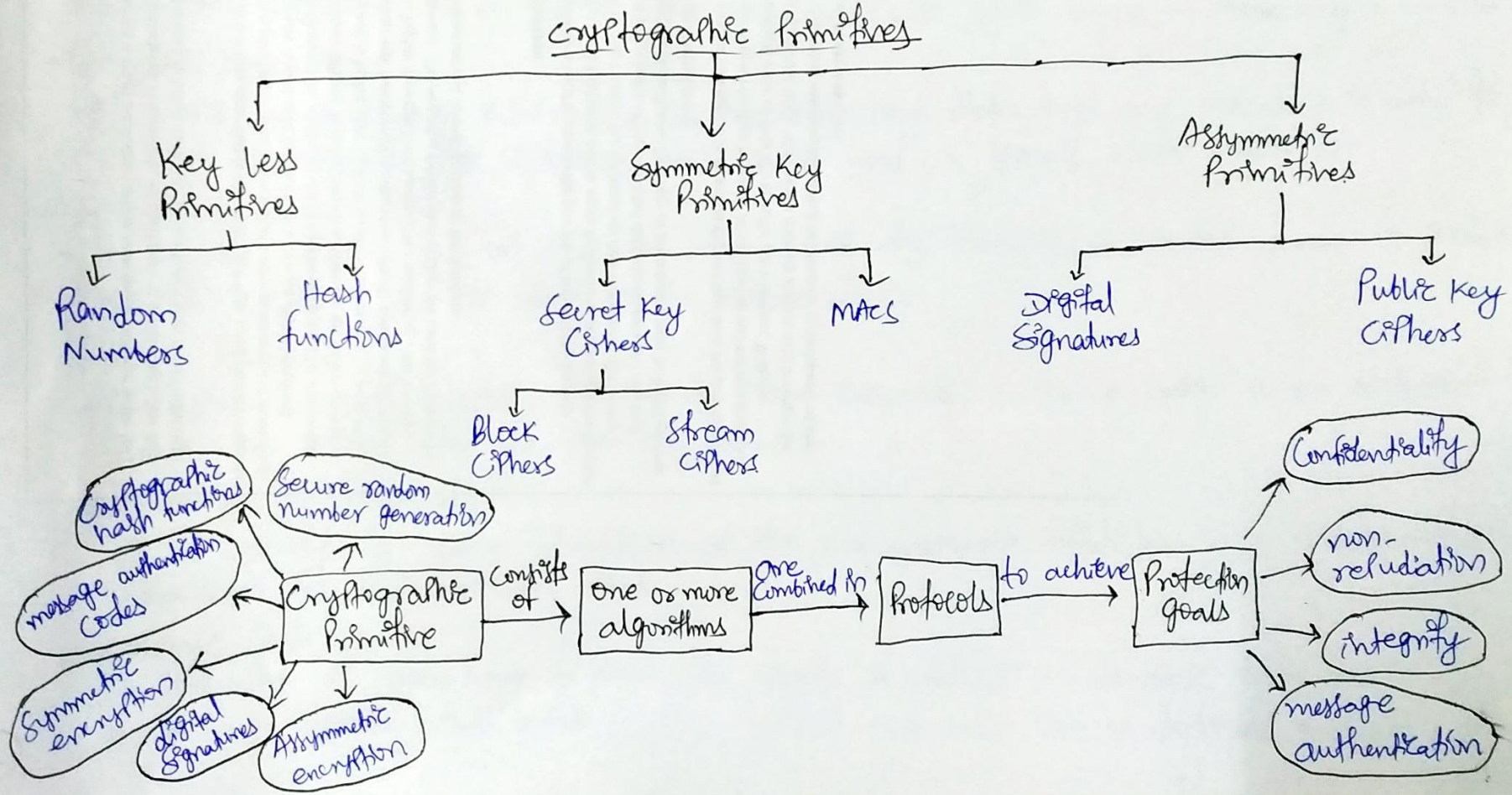
परीक्षार्थी के हस्ताक्षर
Signature of student's

परीक्षक के हस्ताक्षर
Signature of Examiner

Short Answer

Ans 1 Cryptographic Primitives are well-established, low-level cryptographic algorithms that are frequently used to build cryptographic protocols for Computer Security Systems.

- In Simpler terms, we can say that Cryptographic Primitives are basic building-blocks of a Security Protocol or Systems.



Ans 2 Applications of Cryptography

- Authentication/Digital Signatures
  - It is used when someone wants to verify the origin of a document, the identity of the sender, the time and date, of a document was sent and/or signed, and so on.
  - A digital signature is a cryptographic means through which many of these may be verified.
- Encryption/Decryption
  - It works by employing Public Key Cryptography and these keys are required in order to encrypt or decrypt the ciphertext and can be used in email, social media, etc.
- SIM Card Authentication
  - To decide whether or not the SIM may access the network, a random number is generated by the operator, and is sent to the mobile device.
- Storing Passwords
  - Encryption alongwith hashing is used to store passwords, so that a system or an attacker have no access to the plaintext password.
- Reliability in Transmission
  - It is ensured by using checksum of the communicated information and verifying the checksum at the recievers end.
- Electronic Cash
  - Cryptography is used here to keep the assets of nations in electronic form securely.
  - If such systems would be forged, the national economies can be destroyed instantly.

Long Answer

Ans 1

Classical Cipher
- Shift Cipher
- Mono-alphabetic Substitute Cipher
- Poly-alphabetic Substitution (Vigenere Cipher)

(I) Shift Cipher

Encryption - Shift each Plain-text character by 'K' Positions "forward" or vice-versa.

Decryption - Shift each Cipher-text character by 'K' Positions "backward" or vice-versa.

Cryptoanalysis of Shift Cipher
- Plaintext : $m = (m_1, \ldots, m_e)$
- Ciphertext : $c_i = (c_1, --, c_d)$

Attack model : Ciphertext only Attack (COA)

- It is Symmetric cryptosystem as it uses a shared secret.

Information Known to attacker
- Ciphertext
- Process through which the ciphertext is generated, i.e., $C_i = (M_i + \text{Shift}) \bmod 26$

Attack
- Brute force attacks are usually simplest to implement here as there are only 26 Candidate keys.

Frequency Analysis

- As English alphabets have only 26 letters, it is easy to use brute force attack here, but if we use some other alphabet, which has hundreds of characters, it ~~wasn't easy~~ wouldn't be easy to use brute force.
- we compare the frequency of characters by, $\sum_{i=A}^{i=Z} \frac{(C_i - E_i)^2}{E_i}$

Here, C_i = no. of times the ith letter occurred in the ciphertext.

E_i = the expected no. of times the ith letter should occur in a string.

② Mono alphabetic Substitute Cipher

- It fixes the cipher alphabet for a given key.
- This means that every instance of a Plaintext character will encode to the same Ciphertext letter, regardless of the character's position in the Plaintext.
- frequencies are swapped or flattened for more complex substitutions.

Cryptoanalysis

Encryption - Map each Plaintext character to an arbitrary ciphertext character in a one-to-one fashion.

Key - A secret permutation (determined by the key generation algorithm).

Attack - Here, Brute force attack is impractical, as no. of Candidate keys = $26! \approx 2^{88}$.

frequency analysis - Applicable when Plaintext space is a natural language.

Idea - Exploit the redundancy present in the underlying natural language.

③ Polyalphabetic Substitution cipher.

- It uses different alphabets in the encryption process to further diffuse letter frequencies and make decryption harder.
- Provides one-to-many or many-to-many relationship between letters.

Cryptoanalysis

Two stage approach

- Stage 1 - determine the length t of the unknown key.
  - Uses Kasiski's method, Index of Coincidence method.
- Stage 2 - Try to determine the characters $K_1, K_2, \ldots K_t$.

Examples

① Shift cipher

Plain text - ANIKET

Key - 3

Cipher text - DQLNHW

② Mono alphabetic Substitute Cipher

Plain text - ANIKET

Key - WXLSTJPRBCIZKGQDOFEHVNUMAY

Ciphertext - WGBITH

Here, each letter of alphabet is mapped to another letter, hence difficult to implement brute force attack here.

③ Polyalphabetic Substitution Cipher

Plaintext - ANSKET	ANIKET
Key - hge	hgehge
Ciphertext - the rxp	therxp

The best feature of this cipher is that same plaintext character is substituted by different ciphertext characters.

Thus, there were the cryptoanalysis on ~~the~~ some classical ciphers.