Short Answer!-

1:-

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 algorithm
needed to implement a particular security service, ~~a~~ such as encryption
functions or one way hash functions.

→ ~~Gor~~ 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 ~~are~~ rare.

→ Cryptographic primitive are similar to programing languages.

→ It's ~~th~~ 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:-

Aathentication/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/Deoryption 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 generate by the operator and sent to the mobile devices.

Long Answer :-

3:-

Ans:- Classical Cipher:-

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

There are three type: ~~of~~

- → Shift cipher
- → Mono alphabetic Substition cipher
- → Poly-alphabetic substitution (viganare) cipher

#Shift Cipher:- Plain-text and cipher-text character ∈ {a, ..., z}

- Encryption: shift each plain text character by 'k' positions "forward"
- Decryption:- Shift each cipher text character by 'k' positions 'backword'
- k ∈ {0, ..., 25} and randomly selected by the key-genration algorithm

Mathematical interpretation of the shift cipher:-

- interpret the set {a, ..., z} as {0, ..., 25}
- k = {0, ..., 25} and M = C = set of strings over {0, ..., 25}

Exmaple:- Text:- ATTACKATONCE
Shift:- 4
Cipher: EXXEGOEXSRGI

Crypto analysis of shift cipher:-

- Plain text: $m = \{m_1, \ldots, m_l)$
- Chipher text: $c_i = (c_1, \ldots, c_l)$
- Attack model: Ciphertext Only Attack (COA)
  - Infer mation Known to attacker
    - Cipher text
    - Procces through which the ciphertext is generated i.e. $c_1 = (m_1 + k) \bmod 26$
  - Attack
    - An attacker can try to decrypt c with all possible K
    - Easy to mount: only 26 candidate keyes
  - Learning:-
    - Sufficient key space principle:-

Mono Alphabetic Substitute Cipher:-

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

Cryptoanalysis 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 shited based on numeric key

- Idea! exploit the reedundency Present in the underlying natural language.

Poly alphabetic Substitution Cipher:-

- A~~P~~ poly alphaketic cipher is any cipher based on substitution, using multiple substitution alphabets.
- The Vigenere cipher is probtabley the best-known examples of a polyalphabetic cipher. though it is a simplified special case.

Crypto analysis:-

- Two stage approach:-

Stge1:. Determine the length of the unknown key.

- kasicki's methods, Index of coincidence methods

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

- Independent intances of letter frequence analysis

Ex:- Input: Plaintext: GEEKSFORGEEKS
Keyword: AYUSH

Output: Ciphertext: GCYCZFMLYLEIM