Page No.
Date

Devanshu Surana
PC-23, 10322210755
Panel C, Batch C1

ICS Lab A1

FAQ's

1) What are various classical ciphers?
→ They are often divided into transposition and substitution ciphers some examples of classical ciphers are:-
1) Caesar cipher
2) Simple substitution
3) Hill Cipher
4) Polyalphabetic Cipher
5) Monoalphabetic cipher

2) Compare steneography and cryptography:
→ 1) Steganography -
Unknown message passing
Prevents discovery of the very existence of communicati
n.
Little known technology
Technology still being developed for certain formation
once deleted message is known.

2) Cryptography -
Known message passing
Prevents an unauthorized party from discovering the contents
Common technology.

Page No.
Date

most of the algo known by all. Strong current algos are resistant to attack larger expensive computing power is required for cracking

3) State the reason why classical ciphers are absolute.
→ Classical ciphers are absolution due to their vulnerability to frequency analysis. limited key space suspectability to modern computing power. Lack of security for long msgs and the availability of more secure modern cryptographic methods.

4) How to carry cryptoanalysis of classical cryptography.
→ Use frequency analysis to identify common letters symbols.
Look for patterns in the ciphertext
Try guesswork for simple shift cipher
Be prepared for trial and error as you work to decipher the message

5) Write how different disciplines of art, science and engineering have contributed to information security.
→ ART :- used to raise awareness of security issue to educate people about security.

SCIENCE :- Used to develop new security algorithm to identify security vulnerabilities and to design more secure systems.

Page No.
Date

ENGINEERING :- Used to design and build secure systems, to implement security measures and to test security systems.