Cryptanalyst:

Code :

Cipher:

Substitution :

Transposition:

Steganography :

Polyalphabetic Substitution:

Monoalphabetic Substitution:

Block chaining:

Substitution/permutation ciphers:

Viruses, Worms, Trojans…

Hackers, crackers, script kiddies…

A strong cipher system can protect against

cryptanalysis that has much information about the

cipher system. What constitutes this information?

**Major causes of insecurity**

*Complexity*

*Poor coding*

*Technology weaknesses*

*Configuration weaknesses*

*Policy weaknesses*

*Human factors*

Be able to encode or decode a simple transposition or

substitution cipher

Be able to determine keys and encode or decode a

simple RSA cipher

**Back Orifice**

Architecture & Organization

How it might be used

Floods :

Smurfs:

IP Fragmentation :

DoS and DDoS:

Spoofing :

TCP Hijacking:

Buffer overflows:

Man in the Middle:

Replays:

Explain how a certain attack operates

Especially taking advantage of a TCP connection setup

Symmetric encryption vs. Asymmetric encryption

DAC:

HMAC:

Advantages of MACs over hashing

Side info

Unicity distance

Per character language redundancy

**One Time Pads**

Why are they considered unbreakable?

Information entropy concept