Definitions

Thing	Definition
Vulnerability	A flaw or weakness in a system’s design, implementation or operation that could result in a security breach or a violation of the system's security policy
Threat	A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm
Attack	An assault on system security that derives from an intelligent threat.
Risk	Probability that a particular threat will exploit a vulnerability
Non-repudiation	Service can’t deny a message was sent or received
Security Mechanisms	A mechanism that is designed to detect, prevent, or recover from a security attack (Encryption, digital signatures, access controls, data integrity,.. etc)
Fabrication	Attack on authenticity
Distributed consensus protocol	There are n nodes that each have an input value. Some of these nodes are faulty or malicious
Sybil attack	Sybils are just copies of nodes that can be controlled by an adversary
deterministic	repetitions in message may show in ciphertext, using brute force works on this
non-malleable	A cryptosystem where an attacker cannot modify a ciphertext in a way that produces a predictable change in the corresponding plaintext.
Certificate Revocation List (CRL)	a list of the serial numbers of all the certificates revoked by a particular CA, signed by the CA concerned