Review:

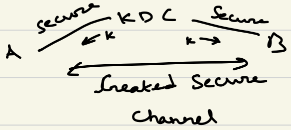
Symmetric-Key Cryptography

Main Primitives Covered:

- Encryption Schemes: Perfect, Ciphertext only attack, CPA secure, CCA secure
- Data Integrity: MAC, CBCMAC, HMAC (today)

Public Key Revolution:

Key Distribution Centers for distributing private keys within an organization of n nodes - 2 people in an n node center does not need to have $O(n^2)$ keys but only 1 - go thorough KDC



Not favoured: KDC can read everything

HMAC:

Consider a family of collision resistant hash function $H^s: \{0,1\}^* \to \{0,1\}^n$

$$t := H^s(\text{opad} \oplus k \,\|\, H^s(\text{ipad} \oplus k \,\|\, m))$$

Fixed, public pads

AES in randomised counter mode + HMAC is CCA secure.

Information vs Knowledge: Knowledge is useful information

Natural Numbers Represented as Infinite symbols

Frequent Operation:

0. No operation
1. Comparison
2. Addition
3. Multiplication

Roman Numerals

Decimal / Binary / ...

$n = \sum_{i=0}^{\infty} d_i B^i$

Tally Marks

Product of primes (Fundamental theorem of arithmetic)

Residue Number System

Choose 2 representations for Key K:

R_{priv}	R_{pub}
$Dec_K()$ Fast	$Enc_K()$ fast
	$Dec_K()$ very slow

Ex: RSA, EL-Gamal, Goldwasser-Micali,

based on integer factorization, DLP

Rabin, Paillier, FHE (Fully Homomorphic Encryption)

Diffie-Hellman

RSA Enc: $m^e \bmod N$

$N = \overset{\text{primes}}{pq}$, $\gcd(e, \phi(N)) = 1$

RSA is a candidate one way fn.

RSA assumption is that RSA is secure