Public key cryptography

Index: A pessimistic theorem, 2 famous relaxations to Shannon's Theory (the magic wand), Limitations of One Time Pad, Catch 22 situation, Fast Secure channels imply fast secure comm. Vernam Cipher cannot convert Slow secure channel + fast insecure channel to a fast secure channel.

(Q1) Can slow secure channel + fast insecure channel create a fast secure channel?

Symm. key cryptography

(Q2) How to get a slow secure channel from scratch?

Symm. Key Cryptography: As long as slow secure channel is not of 0 bandwidth, the bandwidth of fast secure channel is <u>almost</u> as much as fast insecure channel.

Theorem: Perfect secrecy implies $|M| \leq |K|$

The number of bits in the key should be at least as many as in the message. ⇒ The message space should not be compressible ⇒ The slow secure channel used to transfer the key has to transfer at least as many bits as the fast insecure channel used to transfer the message. True even if M is compressible.

Proof: Suppose the contrary is true & $|M| > |K|$ & the scheme is perfectly secure. Given the ciphertext $c \in C$, try decrypting with all keys $k \in K$. This gives a subset of M since $|K| < |M|$. There exists some message $m^* \in M$ ∋ it is not in this subset. Thus, $P[M = m^* \mid C = c] = 0 \neq P[M = m^*]$. Thus, it is not perfectly secure, contradicting our assumption.

∴ Premise holds.

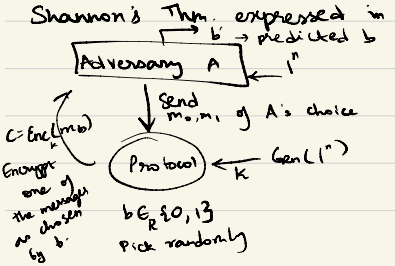
2 necessary relaxations to Shannon's Theory + existence of an 'interesting' mathematical object is sufficient ⇒ One way fn.

Mathematical objects ex: DPL, integer factoring . . . is hard ⇒ generalizes to "If one way fns. exist, the 2 necessary relaxations are sufficient."

⇒ Computational Difficulty class
Computational Indistinguishability class –
Existence of pseudorandom nos, collision resistant hash fns., digital signatures, zero knowledge proof

For (Q1): object is one way fn., for (Q2): trap door one way fn.

Shannon's Thm. expressed in TM:



$\forall$ probabilistic TM A, protocol is perfectly secure if $P[b' = b] \leq 1/2$

Relaxation 1: Only efficient (polynomial time) adversaries need to be tolerated.

↳ in security parameter n

$\Rightarrow$ probabilistic polynomial TM A

Relaxation 2: Negligible probability of error is permitted

Defn.: $\mu(n)$ is said to be negligible in n if $\forall$ polynomials p $\exists$ n_0 $\ni$ $\forall$ $n \geq n_0$

$$\mu(n) \leq \frac{1}{p(n)}$$

Grows slower than every polynomial inverse asymptotically

$\Rightarrow$ $P[b' = b] \leq 1/2 + \text{negligible}(n)$