Review:

Shannon's pessimistic theorem; Perfection implies $|M| \leq |K|$; Huge limitation (impossibility when $|K| = 0$); 2 necessary relaxations conjectured as sufficient: PPTM adversary, negligible error probability

---

Categories of attacks:

- Ciphertext only attack : assumption: pseudorandom generators exist
- Known plaintext attack: ciphertext with corresponding plaintext, & candidate ciphertext
- Chosen plaintext attack - polynomial no. of times & adaptive - can encrypt messages of its choice. Assumption: pseudorandom fns. exist
- Chosen ciphertext attack - can decrypt messages of its choice. Assumption: message authentication codes exist

---

Modern internet does not use a provably secure CCA scheme.

Kinds of encryption schemes: Proven (Ex: One Time Pad), Provable (our approach), Heuristic (most of practice)

Existence of One Way fns. $\Leftrightarrow$ PRG $\Leftrightarrow$ PRF $\Leftrightarrow$ MAC

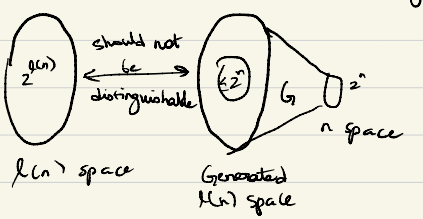
$\Leftrightarrow$ CCA secure encryptions exist $\Leftrightarrow$ CPA sec. $\Leftrightarrow$ CCA sec. enc.

MD5 can be cracked in 22 hours

An enc. scheme is secure against eavesdropping if $P[b' = b] \leq 1/2 + negl(n)$ $\forall$ PPTM A. (See 18 Jan)

$G : \{0,1\}^n \longrightarrow \{0,1\}^{l(n)}$ (deterministic) is a pseudo random generator if (a) Expansion holds: $l(n) > n$ (b) Pseudorandomness: $\forall$ PPTM A, a pseudorandomly generated string of length $l(n)$ should be indistinguishable from a uniformly randomly string of length $l(n)$, i.e.

$$|P(A(U_{l(n)}) = 1) - P(A(G(U_n)) = 1)| \leq negl(n)$$



By pigeonhole principle, using $2^n + 1$ samples, the spaces can be distinguished.
$\Rightarrow$ Prob of repetition in the actual $l(n)$ space is negligible but guaranteed in generated $l(n)$ space, but a PPTM cannot handle an exponential number of samples.

New one time pad: $m \in \{0,1\}^{l(n)}$
$k \in_R \{0,1\}^n$. Enc: $m \oplus G(k)$
Now secure channel is used to send a small key instead of a key of same size as message.
Makes a secure slow channel seem fast.

Pseudorandomness is not a replacement for true randomness.

PRG, part of magic wand : breaks impossibility of $|M| > |K|$. Secrecy provided is indistinguishable from perfect secrecy. Polynomial adversary cannot differentiate b/w 2^n & $2^{l(n)}$ space.

necessary & sufficient

If PRG exists & 2 relaxations are considered, security against eavesdropper is solved. (ciphertext only attack)

Create PRG, from hard problems (NP hard) using one way fns. : either program is secure or adversary has solved NP hard problem in Polynomial time

Win - Win