

Reviews:

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 message of its choice. Assumption: pseudorandom gen. 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 fn. \Leftrightarrow PRG \Leftrightarrow PRF

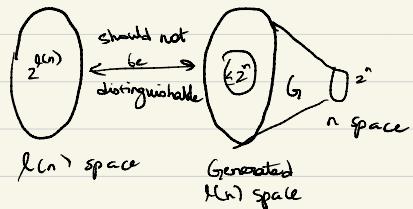
\Leftrightarrow MAC

\Leftrightarrow CCA secure encryptions exist \Leftrightarrow CPA sec.

\Leftrightarrow CCA sec. enc.

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

\rightarrow deterministic
 $G : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ is a pseudo random generator if (a) Expansion holds: $l(n) > n$ (b) Pseudorandomness:
+ PPTM A: a pseudorandomly generated string of length $l(n)$ should be indistinguishable from a uniformly randomly string of length $l(n)$, i.e.
 $|P(A(U_{l(n)})=1) - P(A(G_l(U_n))=1)| \leq \text{negl}(n)$



By pigeonhole principle, using 2^{l+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: $m \in \{0,1\}^{l(n)}$
 $k \in \{0,1\}^n$. 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.

MDS can be cracked in 23 hours

Pseudorandomness is not a replacement for true randomness.

PRG, part of magic wand : to reduce impossibility of $|M| > |K|$. Security provided is indistinguishable from perfect secrecy.
Polynomial adversary cannot differentiate $M \in 2^n$ & $2^{n+o(n)}$ 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