Lecture 02 (Formalizing Definitions)

1 Recap

Saying that AES, SHA etc are building blocks doesn't make sense since it isn't a computational problem but a function

2 Off Topic

2.1 When does Computational Problem become Suitable for Crypto?

Confidence over time - no solution for long

2.2 When does a Computational Problem become NP-Complete?

1. Find reduction from problem to a well known problem
2. It is difficult to compare difficulty of different problems

3 Attempt to Formalize Definition

Adversary should know encryption and decryption function to strengthen the definition

3.1 Adversary should not be able to learn message (given cipher text)

1. $\forall$adversary :

   $$\underset{k \in \mathbb{K}, m \in \mathbb{D}}{P}[A(enc(m,k)) = m] \leq \frac{1}{|m|}$$

   doesn't capture language-ness
2. $\forall$adversary : $\forall$distribution D over M

   $$\underset{k \in \mathbb{K}, m \in \mathbb{M}}{P}[A(enc(m,k)) = m] \leq \min_{x \in M} \underset{m \in D}{P}[m = x]$$

   min does not work since some message might have 0 probability or something
3. $\forall$adversary : $\forall$distribution D over M

   $$\underset{k \in \mathbb{K}, m \in \mathbb{M}}{P}[A(enc(m,k)) = m] \leq \max_{x \in M} \underset{m \in D}{P}[m = x]$$

3.2 Adversary should not be able to learn any predicate on message (given cipher text)

$\forall$adversary : $\forall$distribution D over M :

$$\forall \text{predicate } \phi : \underset{k \in \mathbb{K}, m \in \mathbb{M}}{P}[A(enc(m,k)) = \phi(m)] \leq \max_{b \in \phi(M)} \underset{m \in D}{P}[b = \phi(m)]$$

3.3 Probability Distribution of Message doesn't Change even after seeing Encryption

$\forall$ distribution $D : \forall x \in M : \forall c \in C$

$$\underset{m \in D}{P}[m = x] = \underset{m \in D, k \in K}{P}[m = x | enc(m,k) = c]$$

Example: see Shannon OTP

3.4 Perfect Indistinguishability

$$\forall m_0, m_1 \in M, c \in C : \underset{k \in K}{P}[enc(m_0,k) = c] = \underset{k \in K}{P}[enc(m_1,k) = c]$$

4 Shannon One Time Pad

$$M = K = C = \{0,1\}^n$$
$$enc(m,k) = m \oplus k$$
$$dec(c,k) = c \oplus k$$

4.1 Does it Satisfy Definition 3?

$D =$ uniform over M

$$\underset{m \in D}{P}[m = x] = \frac{1}{|M|}$$
$$\forall c \in C : \underset{m \in D, k \in K}{P}[m = x | m \oplus k = c] = \frac{1}{|M|}$$

Yes, it satisfies definition!

4.2 Does it Satisfy Definition 4?

$$\underset{k \in K}{P}[enc(m,k) = c] = \frac{1}{|K|}$$

Yes!

5 Exercise - for a coffee

Compare the first three definitions and show equivalence or strength of definitions