Stream Cipher

0.1 Symmetric Ciphers

Definition 1. ***Cipher***: *a cipher defined over* $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ *is a pair of "efficient" algs* (E, D) *where* $E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C},\ D : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$ *s.t* $\forall m \in \mathcal{M}, k \in \mathcal{K},\ D(k, E(k, m)) = m$

Definition 2. ***One Time Pad***: $\mathcal{M} = \mathcal{C} = \{0, 1\}^n,\ \mathcal{K} = \{0, 1\}^n,\ c = E(k, m) = k \oplus m,\ D(k, c) = k \oplus c.$

Definition 3. *Shannon(1949): A cipher* (E, D) *over* $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ *has* ***perfect secrecy*** *if* $\forall m_0, m_1 \in \mathcal{M}(len(m_0)len(m_1))$ *and* $\forall c \in \mathcal{C}$

$$Pr[E(k, m_0) = c] = Pr[E(k, m_1) = c]$$

Where k *is uniform in* $\mathcal{K}$.

Lemma 1. *One Time Pad has prefect secrecy.*

Theorem 1. *Perfect secrecy implies key length* $\geq$ *message length.*

0.2 Stream Ciphers

idea: replace "random" key with PRG(pseudorandom) key.

Definition 4. *PRG:* $G : \{0, 1\}^s_{(seed\ \ space)} \rightarrow \{0, 1\}^n,$ *where* $n >> s$ *and*

$$c = E(k, m) = m \oplus G(k)\ ,\ m = D(k, c) = c \oplus G(k)$$

Definition 5. *Predictability: a PRG, $G : \mathcal{K} \to \{0,1\}^n$ is **predictable** if $\exists$ efficient algorithm A and $1 \le i \le n-1$ s.t*

$$Pr\left[A(G(k)|_{1,\ldots,i}) = G(k)|_{i+1}\right] \ge \frac{1}{2} + \epsilon$$

where k is uniform on $\mathcal{K}$, for some non-negligible ϵ.

Definition 6. *Unpredictability: a PRG is **unpredictable** if it is not predictable: $\forall i$, no efficient algorithm can predict $i+1$ bit for non-negligible ϵ.*

Definition 7. *$\epsilon : \mathbb{Z}^{\ge 0} \to \mathcal{R}^{\ge 0}$ is non-negligible if $\exists d : \epsilon(\lambda) \ge \frac{1}{\lambda^d}$ infinitely often.*

0.3 Security of PRG

Definition 8. *a **Statistical Test** on $\{0,1\}^n$ is an algorithm A such that $A(x) \in \{0,1\}$ (0 denotes x is not random, 1 denotes random)*

Definition 9. ***Advantage** of PRG:*

$$Adv_{PRG}[A,G] = \Big| Pr[A(G(k)) = 1] - Pr[A(r) = 1] \Big| \in [0,1]$$

where r is truely random on $\mathcal{K}$ (uniform).
$Adv \to 1$ means A can distinct G from random.
$Adv \to 0$ means A cannot distinct G from random.

Definition 10. *$G : \mathcal{K} \to \{0,1\}^n$ is **secure** PRG if for all efficient statistical tests A, $Adv_{PRG}[A,G]$ is negligible.*

Theorem 2. *PRG predictable iff PRG is insecure. PRG unpredictable iff PRG is secure.*

Definition 11. *Let P_1, P_2 be two distributions over $\{0,1\}^n$. P_1 and P_2 are computationally indistinguishable denoted by $P_1 \approx_p P_2$ if for all efficient statistical tests A*

$$\Big| Pr_{k \leftarrow P_1}[A(k) = 1] - Pr_{k \leftarrow P_2}[A(k) = 1] \Big| < neg$$

Lemma 2. *A PRG is secure if*

$$\{G(k) \mid k \leftarrow \mathcal{K}\} \approx_p uniform(\{0,1\}^n)$$