Perfect security:

Monday, 14 September 2020 12:30 PM

$A : X \to Y$.

$A(x) = y$ is an event.

$Pr(A(x) = y)$.

Dist. induced by x on Y.

If we have a distribution on input X. $Pr(X = x)$.

A induces a joint distri.

$$A_{XY} = Pr(X = x_i, Y = y_j) \parallel$$
$$= Pr(X = x_i) \cdot Pr(A(x_i) = y_j)$$

$$\to Pr(A(x_i) = y_j)$$
$$= Pr(Y = y_j \mid X = x_i)$$

$X = \{x_1, x_2 \ldots x_n\}$.

$Y = \{y_1, y_2 \ldots y_m\}$.

$$Pr(X = x_i, Y = y_j) = Pr(X = x_i) \cdot Pr(Y = y_j \mid X = x_i)$$

$M \to Pr(M = m)$.

$E(K, M) \to C$.

$Pr(C = c \mid M = m) = Pr(C = c)$.

$Pr(M = m \mid C = c) = \underline{Pr(M = m)}$.

If the encryption is perfectly secure, then M & C are independant.

$$Pr(M = m, C = c)$$
$$= Pr(M = m) \cdot Pr(C = c)$$
$$= Pr(M = m) \cdot Pr(E(m) = c)$$

(by Def)

Dist on M & K are independant. (Reasonable assumption)

Distinguishability:

Plaintext - lots of 2 - len 2

$c \to$ even of 1

c - odd - 1

$m_0 \to 0 \cdots 0$

$m_1 - 1 \cdots 1$

Semantic Security:

A $\xrightarrow{m_0, m_1}$ C

$\xleftarrow{c = E(m_0)}$

$$Pr(A(m_0, m_1, c) = m_0) : c \leftarrow E(m_0)$$
$$= Pr(A(m_0, m_1, c) = m_1) : c \leftarrow E(m_0)$$

$$Pr(A(m_0, m_1, c) = m;\ m \xleftarrow{u} \{m_0, m_1\},\ c = E(m)\}$$
$$= \frac{1}{2}.$$

1000, 1

1000, 740, 1,

1000, 740, 60

29, 31

$n = 1000$ n

n headed die:

$n = 1$ step.

$a < p$, if p is a prime:

$a^{p-1} \equiv 1 \mod p$.

---

n is prime or not.

Randomly choose a

$a < n$.

$a^{n-1} \equiv 1 \mod n$?

$\therefore n$ is prime.

$a^{n-1} \not\equiv 1 \mod n$.

n is NOT prime — correct.

$n = 15$. $4^2 \equiv 1 \mod 15$

$a = 4$

$4^{14} \equiv 1 \mod 15$.

$$Pr(A(m_0, m_1, c) = m) \quad c = E(m)$$

$m \leftarrow \{m_0, m_1\}$

$$\frac{1}{2}.$$

$$Pr(m, c, A(c) = m)$$
$$= Pr(m, c) \cdot Pr(A(c) = m).$$
$$Pr(m) \cdot Pr(E(m) = c)$$

Prob. of Success of Adversary:

$$Pr(M = m, C = c)$$
$$= Pr(M = m) \cdot Pr(E(m) = c).$$

~~When $A(c) = m$ A had succeeded iff the event $E(m) = c$ should have happened, m was.~~

When $A(C) = m$,

A is said to have Succeeded iff.

(a) m is chosen for enc.

(b) $E(m) = c$.

$$Pr(\text{Success of } A)$$
$$= \sum_{m, c} Pr(m) \cdot Pr(E(m) = c) \cdot Pr(A(c) = m).$$

$$= \sum_{m, c} Pr(m) \cdot \underbrace{Pr(c)}_{\alpha} \cdot Pr(A(c) = m)$$

$$= \sum_c Pr(c) \cdot \sum_m Pr(m) \cdot Pr(A(c) = m)$$

Let $\alpha = Max\ Pr(m)$.

$$\le \alpha \sum_c Pr(c) \cdot \sum_m Pr(A(c) = m).$$
$$= \alpha \cdot 1 \cdot 1.$$

$$\underline{Pr(\text{Success for } A) \le \alpha}.$$

$$Max\{Pr(M = m)\}$$

$M = \{1, 2, 3, 4\}$

$\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8}$.

$= \left\{\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\right\}$

$\{H, T\}$

$.8, .2$

$\{.5, .5\}$

$c = m \oplus k$.

If same secret key is used twice, then the perfect se. can not be maintained.

Entropy of a Distribution:

$E(m)$

Randomly choose k.

$c = m \oplus k$.

$\frac{1}{2^n} \longrightarrow \frac{f(n)}{2^n}$

$\frac{Poly}{exp} <$.

$.0000001$

2

Delfs & Knebl: Int. Cryp.

pp 290 - 291 - 292

3rd edition