Probability

1) State space Ω
2) Event space $\mathcal{F} \subseteq 2^{\Omega}$
   (For us, $\mathcal{F} = 2^{\Omega}$)
3) $P : 2^{\Omega} \to [0,1]$

Bayes's Thm

$$P(E|F) = \frac{P(F|E)P(E)}{P(F)}.$$

A Random Variable is a fn $X : \Omega \to \mathbb{R}$

events like, for $x \in \mathbb{R}$

$$\{\omega \in \Omega \mid X(\omega) \le x\}$$

pdf: $f_X(x) = P(X = x)$

$$= P(\{\omega \in \Omega \mid X(\omega) = x\})$$

We can start w/ pdf and get P

Ex: uniform distribution on S w/ n elts given by X satisfying $f_X(j) = 1/n$ if $j \in S$.

Ex: binomial distribution:

$$f_X(k) = \binom{n}{k} p^k (1-p)^{n-k} = \frac{n!}{k!(n-k)!} p^k (1-p)^{n-k}$$

Dfn: Let X be a RV

outputs are $x_1, \dots, x_n$.

Then the expected value of X (or mean) is

$$\mathbb{E}(X) = \sum_{\omega \in \Omega} X(\omega)\, P(\{\omega\})$$

$$= \sum_{i=1}^{n} x_i \cdot P(X = x_i)$$

$$= \sum_{i=1}^{n} x_i\, f_X(x_i)$$

rolling a die

$$\mathbb{E}(X) = \frac{1}{6}(1) + \frac{1}{6}(2) + \frac{1}{6}(3) + \frac{1}{6}(4) + \frac{1}{6}(5) + \frac{1}{6}(6)$$

$$= \frac{7}{2}$$

§2.2 Information Theory

Dfn: A (symmetric) crypto system is

- A set $\mathcal{M}$ of messages
- A set $\mathcal{C}$ of ciphertexts
- A set $\mathcal{K}$ of keys
- encryption function $e: \mathcal{K} \times \mathcal{M} \to \mathcal{C}$
- decryption fn $d: \mathcal{K} \times \mathcal{C} \to \mathcal{M}$

s.t. $d(k, e(k,m)) = m$

$e(k, d(k,c)) = c$

often fix $k \in \mathcal{K}$, and set

$e_k(m) = e(k,m)$

$d_k(c) = d(k,c)$.

$d_k = e_k^{-1}$.

the function e_k is 1-1.

When is this any good?

- given k, m, easy to compute $e(k, m)$.
- given k, c, easy to compute $d(k, c)$
- given a set of $c_i \in \mathcal{C}$, hard to find $d_k(c_i)$ w/o k.
- given a collection of pairs (m_i, c_i), hard to decrypt a new ciphertext.

Kerckhoff's principle

"should not require secrecy, and it should not be a problem if it falls into enemy hands."

Shannon's Maxim

"the enemy knows the system."

§2.2.1 Perfect Secrecy

Dfn: a crypto system has <u>perfect secrecy</u> if

$$P(m|c) = P(m)$$

$\forall\, m \in \mathcal{M},\ c \in \mathcal{C}$.

Bayes:

$$P(a|b)\,P(b) = P(b|a)\,P(a)$$

$$\cancel{P(m|c)}\,P(c) = P(c|m)\,\cancel{P(m)}$$

$$\Rightarrow\ P(c) = P(c|m)$$

Ex: $\mathcal{K} = \{k_1, k_2\}$

$\mathcal{M} = \{m_1, m_2, m_3\}$, $\mathcal{C} = \{c_1, c_2, c_3\}$

	m_1	m_2	m_3
k_1	c_2	c_1	c_3
k_2	c_1	c_3	c_2

$P(m_1) = P(m_2) = 1/4$, $P(m_3) = 1/2$

assume $P(k_1) = P(k_2) = 1/2$

$$P(c_2) = P(m_1)P(k_1) + P(m_3)P(k_2)$$

$$= \frac{1}{4}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{2} = 3/8$$

$P(c_2|m_2) = 0 \neq 3/8$ no PS.

Prop: If PS, then
$\# \mathcal{K} \geq \# \mathcal{M}$.

Pf/ fix some $c \in \mathcal{C}$ w/
$P(c) > 0$.
$P(c \mid m) = P(c) \ \forall m \in \mathcal{M}$,
so $P(c \mid m) > 0 \ \forall m \in \mathcal{M}$.

$\forall m \in \mathcal{M}, \exists k \in K$ s.t. $e(k, m) = c$

suppose $e(k, m_1) = e(k, m_2) = c$.
$d(k, c) = m_1$
$d(k, c) = m_2$ so $m_1 = m_2$.

So distinct key for each $m \in \mathcal{M}$.

Thus $\# K \geq \# \mathcal{M}$.