CIS 5371 Cryptography

3. Probability & Information Theory

Basic rules of probability

Notation

- Events: $S, \varnothing, E, F, \ldots, E \cup F, E \cap F, \ldots$
- . $\overline{E} = S \setminus E, \quad \Pr[\overline{E}] + \Pr[E] = 1$
- $\Pr[S]=1, \Pr[\varnothing]=0, \quad 0 \le \Pr[E] \le 1$
- $\Pr[E \cup F] = \Pr[E] + \Pr[F] - \Pr[E \cap F],$
- . $E \subseteq F \quad \Rightarrow \quad \Pr[E] \le \Pr[F]$
- . $\Pr[F \mid E] = \dfrac{\Pr[E \cap F]}{\Pr[E]}$

Basic rules of probability

An Experiment can yield one of *n* equally probable outcomes.

- Event E1: One of the *n* values occurs.
- Pr[E1] = 1/*n*
- Event E2: *m* of the *n* values occur.
- Pr[E2] = *m*/*n*
- Event E3: *An Ace is drawn from a pack of 52 cards*
- Pr[E3] = 4/52 = 1/13

Basic rules of probability

Binomial Distribution:

$$\Pr[k \text{ succeses in } n \text{ trials}] = \binom{n}{k} p^k (1-p)^{n-k}$$

Bayes' Law:

$$\Pr[E \mid F] = \Pr[F \mid E] \frac{\Pr[E]}{\Pr[F]}$$

Birthday Paradox

Let $f : X \to Y$ *where* Y *is a set of* n *elements*

Event $E_{k,\varepsilon}$:

for k *pairwise distinct values* $x_1, x_2, \ldots, x_k$ *the probability of a collision* $f(x_i) = f(x_j)$, *occurs for some* $i \neq j$, *is at least* ε

Birthday Paradox : If $\varepsilon = 1/2$ *then* $k \approx 1.1774\sqrt{n}$

Information Theory

Entropy (Shannon)

- The entropy of a message source is a measure of the amount of information the source has
- Let $L = \{a_1, \ldots, a_n\}$ be a language with n letters.
- S is a source that outputs these letters with independent probabilities Prob[a_1], … , Prob[a_n].
- The entropy of S is:

$$H(S) = \sum_{i=1}^{n} \Pr[a_i] \log_2 \left(\frac{1}{\Pr[a_i]} \right) \ bits$$

Information Theory

Example

A source S outputs a random bit.

Its entropy is:

$$H(S) = \Pr[0]\log_2\left(\frac{1}{\Pr[0]}\right) + \Pr[1]\log_2\left(\frac{1}{\Pr[1]}\right)$$

$$= \frac{1}{2}(1) + \frac{1}{2}(1) = 1\,bit$$