Shannon's Theory for Secure Communication

Guevara Noubir
http://www.ccs.neu.edu/home/noubir/Courses/CSG252/F04

Textbook: "Cryptography: Theory and Applications",

Douglas Stinson, Chapman & Hall/CRC Press, 2002

Reading: Chapter 2

Outline

- Recap of elementary probability theory
- Perfect secrecy
- Entropy
- Spurious keys & unicity distance
- Product cryptosystems

Basic Probability Theory

- Discrete random variable: X
  - Finite set X,
  - Probability distribution function s.t. $\Pr[x] \geq 0$ $\sum_{x \in X} \Pr[x] = 1$
  - Example:
    - Probability that the sum of a pair of dice is 4
- Joint Probability of X, and Y: Pr[x, y]
- Conditional Probability: Pr[x | y]
- Independent variables
- Bayes' Theorem (Pr[y]>0):
- Corollary: characterizing independent variables

Approaches to Security

- Computational Security
  - If the best algorithm for breaking it requires at least a very large (specified) number of operations
  - Usually against some specific type of attacks (e.g., exhaustive key search)
- Provable Security
  - Reduction to a well-studied problem. Only relative proof!
  - Example: secure if a given number cannot be factored
- Unconditional Security
  - No bound placed on the computation capability of the adversary

Perfect Secrecy

- Assumption:
  - A cryptographic key is used for only one encryption
  - Probability distribution function on the key
  - Probability distribution function on the plaintext
  - Key and Plaintext are independent random variables
- Observations:
  - Pdf on P, K induces pdf of C
  - Pr[y|x] =
  - Pr[x|y] =
- Example:
  - P = {a, b}, Pr[a] = ¼; Pr[b] = 3/4,
  - K = {k_1, k_2, k_3} with Prob. ½, ¼, ¼
  - C = {1, 2, 3, 4}
  - Pr[1], …? Pr[a|1], …Pr[b|1], …?

	a	b
k_1	1	2
k_2	2	3
k_3	3	4

Perfect Secrecy

- A cryptosystem has perfect secrecy if
  - Pr[x|y] = Pr[x], for all x ∈ X, y ∈ Y
- A posteriori probability that the plaintext is x given the ciphertext is equal to the apriori probability
- Theorem (shift cipher perfect secrecy):
  - The shift cipher where the all keys have probability 1/26, has perfect secrecy (for any plaintext probability).
- Theorem (characterizing perfect secrecy cryptosystems):
  - Let (P, C, K, E, D) be a cryptosystem where |K| = |P| = |C|
  - This cryptosystem has perfect secrecy iff all keys have the same probability 1/|K|, and $\forall x \in P, y \in C, \exists_1 k \in K; e_k(x) = y$
- Vernam's Cipher perfect secrecy

Entropy

- Measure of uncertainty (in bits) introduced by Claude Shannon in 1948 [Information Theory]
- H(x) =
- Example 1:
  - $Pr[x_1] = ½; Pr[x_2] = ¼; Pr[x_3] = ¼$
- Example 2:
  - H(P) = 0.81
  - H(K) = 1.5
  - H(C) = 1.85

Huffman Encoding

- Entropy of a string provides the minimum average number of bits required to encode a random source
- Huffman Encoding provides the rules allow an encoding with less that H(X) + 1 bits on average

Properties of Entropy

- Concave function:
- Strictly concave function:
- Jensen's inequality:
- Theorem:
  - X: random variable that can take *n* values with non-zero probability
  - $H(X) \leq \log_2 n$
  - Equality?

Entropy (Cont.)

- $H(X, Y) \leq H(X) + H(Y)$
- Conditional Entropy:
  - $H(X|y) =$
  - $H(X|Y) =$
- $H(X, Y) = H(Y) + H(X|Y)$
- $H(X|Y) \leq H(X)$ (when do we have equality?)

Spurious Keys and Unicity Distance

- Key equivocation: $H(K|C)$
- Definition:
  - Spurious key is a key possible but incorrect key
- Example:
  - Shift cipher: ciphertext = *WNAJW*
  - Plaintext can: *river* (k=5) or *arena* (k=22)
- Goal:
  - Find a bound on the number of spurious keys
- Theorem:
  - $H(K|C) = H(K) + H(P) - H(C)$
  - Example:
    - $H(P) = 0.81$, $H(K) = 1.5$, $H(C) = 1.85$
    - $H(K|C) = 0.46$: also verified manually

Entropy of a Language

- Number of information bits per letter: H_L
- Example:
  - If all letters have the same probability, a first approximation would be: ≈ 4.7
  - A *first-order* approximation of English language gives H(P) = 4.19
  - *Second-order* approximation, …
- Definition:
  - The entropy of a language *L* is: $H_L = \lim_{n \to \infty} \frac{H(P^n)}{n}$
  -
  - The redundancy of a language *L* is: $R_L = 1 - \frac{H_L}{\log_2 |P|}$
- English has $1 \leq H_L \leq 1.5$
- Redundancy ≈ 0.75

Unicity Distance

- Theorem:
  - Suppose (P, C, K, E, D) is a cryptosystem where |C| = |P| and the keys are chosen equiprobably. Let R_L be the redundancy of the underlying language. Then given a string of ciphertext of length *n*, the expected number of spurious keys satisfies:

$$\overline{s_n} \geq \frac{|K|}{|P|^{nR_L}} - 1$$

- Definition:
  - The unicity distance of a cryptosystem is the value n_0 after which the expected number of spurious keys becomes 0.
  - It is the average amount of ciphertext required for an opponent to be able to compute the key (given enough computing time).
- Example:
  - Substitution cipher: $n_0 \approx 25$
  - For the substitution cipher on average the opponent needs at least a ciphertext of length 25

Product Cryptosystems [Shannon 49]

- Goal:
  - Combine two cryptosystems to obtain a more "secure" cryptosystem
- Product of *Endomorphic* cryptosystem: P = C
  - $S_1 = (P, P, K_1, E_1, D_1)$; $S_2 = (P, P, K_2, E_2, D_2)$
  - Product cryptosystem $S_1 x S_2 = (P, P, K_1 x K_2, E, D)$ s.t. for ever key $k=(k_1, k_2)$: $e_{(k1,k2)}(x) = e_{(k2)}(e_{(k1)}(x))$
  - $d_{(k1,k2)}(x)$ = ?
  - Probability distribution: $Pr[(k_1, k_2)] = Pr[k_1] x Pr[k_2]$

Product of Cryptosystems

- Example:
  - Multiplicative cipher (M):
  - Key space: ?
  - Multiplicative Cipher x Shift Cipher: MxS = ?
  - SxM = MxS = ?
  - Property:
    - S and M commute but this does not hold for all cryptosystems
- The product operation is Associativity
  - Derives from ?

Product of Cryptosystems

- Definition:
  - SxS = S^2
  - SxSx…xS = S^n (n times)
  - If S = S^2 then S is called idempotent
    - Examples: Shift cipher, Substitution, Affine, Hill, Vigenere
- Rule:
  - If a cryptosystem is idempotent: there no security increase by iterating (S^n)
  - If a cryptosystem is not idempotent: security can be increased by iteration
    - Example: Data Encryption Standard
- Constructing non idempotent cryptosystems:
  - product of two different simple cryptosystems
  - Is there any obvious property that the two cryptosystems need to satisfy for the product not to be idempotent?
  - Example: product of substitution ciphers by permutation ciphers