Cryptography CS 555

Lecture 3: One-time Pad and Perfect Secrecy

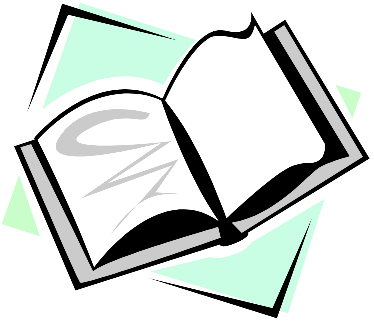
Department of Computer Sciences

Purdue University

Lecture Outline

- Elements of probability theory
- Perfect secrecy
- One-time pad
- Entropy

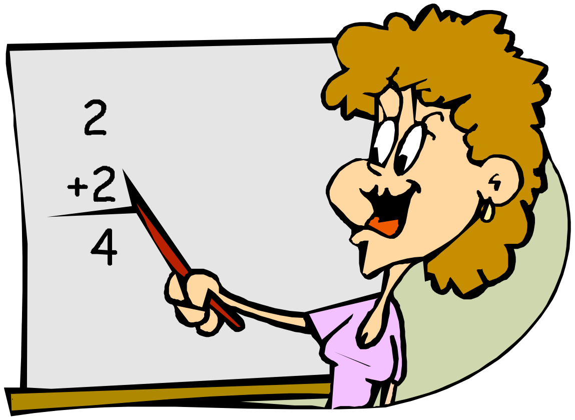
Recommended Reading



- Stinson, Chapter 2

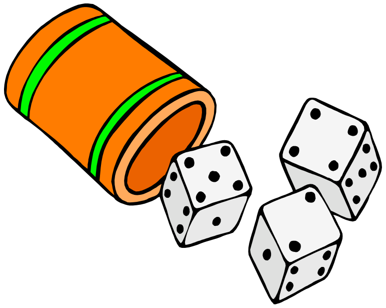
- **Additional Reading**.
  - C. E. Shannon, “Communication Theory of Secrecy Systems”, Bell System Technical Journal, vol.28-4, pp 656--715, 1949.

Begin Math



Elements of Probability Theory

A random experiment has an unpredictable outcome.



Definition

The sample space (S) of a random phenomenon is the set of all outcomes for a given experiment.

Definition

The event (E) is a subset of a sample space, an event is any collection of outcomes.

Basic Axioms of Probability

If E is an event, *Pr(E)* is the probability that event E occurs then

(a) 0 □ Pr(A) □ 1 for any set ***A in S***.

(b) Pr(S) = 1 , where S is the sample space.

(c) If E_1, E_2, … E_n is a sequence of mutually exclusive events, that is Ei□Ej = 0, for all ***i*** $\neq$ ***j*** then:

$$\Pr(E_1 \cup E_2 \cup ... \cup E_n) = \mathop{\square}_{i=1}^{n} \Pr(E_i)$$

Probability: More Properties

If E is an event and *Pr(E)* is the probability that the event E occurs then

- *Pr(Ê)* = 1 - *Pr(E)* where Ê is the complimentary event of E
- If outcomes in S are equally like, then

  Pr(E) = |E| / |S| (where | | denotes the cardinality of the set)

Example

Random throw of a pair of dice.
What is the probability that the sum is 3?

Solution: Each dice can take six different values {1,2,3,4,5,6}. The number of possible events (value of the pair of dice) is 36, therefore each event occurs with probability 1/36.

Examine the sum: 3 = 1+2 = 2+1
The probability that the sum is 3 is 2/36.

What is the probability that the sum is 11?

Random Variable

Definition

A **discrete random variable, X,** consists of a finite set X, and a probability distribution defined on X. The probability that the random variable **X** takes on the value x is denoted **Pr**[**X** =x]; sometimes, we will abbreviate this to **Pr**[x] if the random variable **X** is fixed. It must be that

$$0 \le \Pr[x] \quad \text{for all } x \in X$$

$$\sum_{x \in X} \Pr[x] = 1$$

Relationships between Two Random Variables

Definitions

Assume X and Y are two random variables, we define:

- joint probability: **Pr**[x, y] = **Pr**[x|y] Pr[y] is the probability that X takes value x and Y takes value y;.

- conditional probability: **Pr**[x|y] is the probability that X takes on the value x given that Y takes value y.

- independent random variables: X and Y are said to be independent if **Pr**[x,y]=**Pr**[x]P[y], for all x X and all y Y.

Elements of Probability Theory

Bayes’ Theorem

If Pr[y] > 0 then

$$\Pr[x \mid y] = \frac{\Pr[x]\Pr[y \mid x]}{\Pr[y]}$$

Corollary

X and Y are independent random variables
iff Pr[x|y] = Pr[x], for all x X and all y Y.

End Math

}

Symmetric Ciphers

Plaintext: data to be encrypted

Ciphertext: encrypted data

Same key used for encryption and decryption

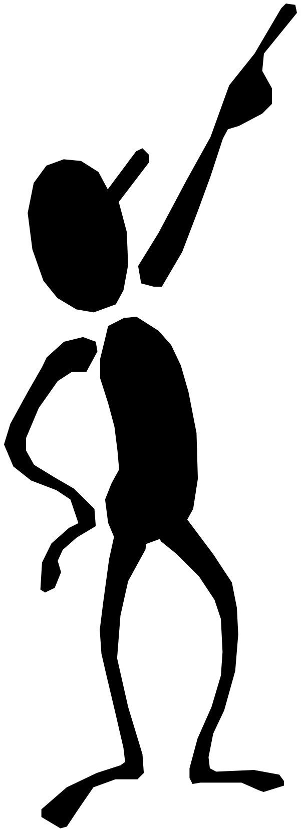
Definition

A **cypher** is a five-tuple (□, C, K, E, D), s. t.:

1. P is a finite set of possible plaintexts
2. C is a finite set of possible ciphertexts
3. K, the keyspace, is the set of possible keys
4. For each k□K, there are
    - encryption rule e_k, e_k:P □ C,
    - decryption rule d_k, d_k:C □ P,
    - s.t. $d_k(e_k(x)) = x$

– □ k□K $\mathbf{e}_k[\ ]$: P □ C must be a one-to-one function

Kerckhoff's Principle



- What can we say about the security guarantees of a cryptosystem?

Kerckhoffs's Principle

- The security of a cryptosystem must not depend on keeping secret the crypto-algorithm.
- The security should depend only on keeping secret the key.

Cryptanalysis Revisited

- Goals:
  - recover encryption key
  - decrypt one message
- Attack models:
  - ciphertext only,
  - known plaintext,
  - (adaptive) chosen plaintext,
  - (adaptive) chosen ciphertext

Approaches to Security

- The attacker has unlimited resources: analysis based on probability theory.
- The attacker has limited resources: analysis based on complexity theory.
- Proofs/guarantees with respect to a specific attack.
- Security against one type of attack, does not guarantee security against other types of attacks.
- WHAT IS THE MEANING OF “SECURE”?

Unconditional Security

- The adversary has unlimited computational resources.
- Analysis is made by using probability theory.
- Perfect secrecy: observation of the ciphertext provides no information to an adversary.
- Result due to Shannon, 1949.

  C. E. Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal, vol.28-4, pp 656--715, 1949.

Ciphers Modeled by Random Variables

Consider a cipher (P, C, K, E, D). We assume that:

1. there is a probability distribution on the plaintext (message) space
2. the key space also has a probability distribution. We assume the key is chosen before the message, the key and the plaintext are independent random variables
3. the ciphertext is also a random variable

Example

P = plaintext

C = ciphertext

K = key

P: {a, b};

Pr(a) = 1/4; Pr(b) = 3/4

K: {k1, k2, k3};

Pr(k1) = 1/2; Pr(k2) = Pr(k3) = 1/4

C: {1,2,3,4};

$e_{k1}(a) = 1$; $e_{k1}(b) = 2$;

$e_{k2}(a) = 2$; $e_{k2}(b) = 3$;

$e_{k3}(a) = 3$; $e_{k3}(b) = 4$;

Perfect Secrecy

Definition

Informally, perfect secrecy means that an attacker can not obtain any information about the plaintext, by observing the ciphertext.

What type of attack is this?

Definition

A cryptosystem has perfect secrecy if **Pr[x|y] = Pr[x], for all x □ P and y □ C**, where P is the set of plaintext and C is the set of ciphertext.

Details

P = plaintext

C = ciphertext

K = key

Bayes: $\Pr[x \mid y] = \dfrac{\Pr[x]\Pr[y \mid x]}{\Pr[y]}$

C(k): the set of all possible ciphertexts if key is k.

$\Pr[y] = \sum_{K:y \in C(k)} \Pr[k]\Pr[x]$ and $\Pr[y \mid x] = \sum_{K:x=d_k(y)} \Pr[k]$

$$\Pr[x \mid y] = \frac{\Pr[x] \sum_{K:x=d_k(y)} \Pr[k]}{\sum_{K:y \in C(k)} \Pr[k]\Pr[x]}$$

Example

P: {a, b}; Pr(a) = 1/4; Pr(b) = 3/4

K: {k1, k2, k3}; Pr(k1) = 1/2; Pr(k2) = Pr(k3) = 1/4

C: {1,2,3,4}; $e_{k1}(a) = 1$; $e_{k1}(b) = 2$; $e_{k2}(a) = 2$; $e_{k2}(b) = 3$;
$e_{k3}(a) = 3$; $e_{k3}(b) = 4$;

Distribution of the ciphertext:

Pr(1) = Pr(k1)Pr(a)=1/2 * 1/4 = 1/8

Pr(2) = Pr(k1)P(b) + Pr(k2)Pr(a) = 1/2 * 3/4 + 1/4 *1/4 = 7/16

Similarly: Pr(3) = 1/4; Pr(4) = 3/16;

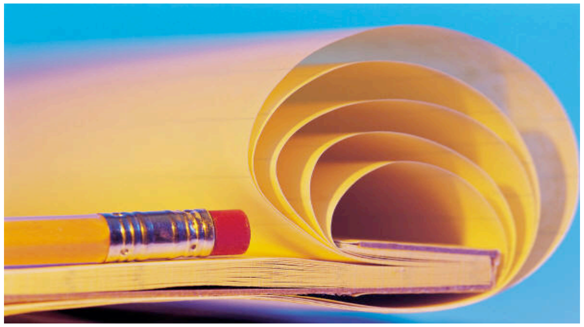
Conditional probability distribution of the ciphertext (we use Bayes)

Pr(a|1) = Pr(1|a)Pr(a)/Pr(1) = 1/2*1/4/(1/8) = 1

Similarly: Pr(a|2) = 1/7; Pr(a|3) = 1/4; Pr(a|4) = 0;
Pr(b|1) = 0; Pr(b|2) = 6/7; Pr(b|3) = 3/4; Pr(b|4) = 1

DOES THIS CRYPTOSYSTEM HAS PERFECT SECRECY?

One-Time Pad



$X = Y = K = (Z_2)^n$

$X = (x_1\ x_2\ \ldots\ x_n)$

$K = (k_1\ k_2\ \ldots\ k_n)$

$Y = (y_1\ y_2\ \ldots\ y_n)$

$e_k(X) = (x_1+k_1\ \ x_2+k_2\ \ldots\ x_n+k_n) \bmod 2$

$d_k(Y) = (y_1+k_1\ \ y_2+k_2\ \ldots\ y_n+k_n) \bmod 2$

One-time Pad has Perfect Secrecy

- One time pad: $P = C = K = \{0,1\}^n$, key is chosen randomly

Proof: for any probability of the plaintext,

$$\forall x \; \forall y \;\; \mathbf{Pr}[x \mid y] = \mathbf{Pr}[x, y] \; / \; \mathbf{Pr}[y]$$

$$= \mathbf{Pr}[x] \, \mathbf{Pr}[y \mid x] \; / \; \sum_{x \in X} (\mathbf{Pr}[x] \, \mathbf{Pr}[y \mid x])$$

$$= \mathbf{Pr}[x] \, 1/2^n \; / \; \sum_{x \in X} (\mathbf{Pr}[x] \, 1/2^n)$$

$$= \mathbf{Pr}[x] \; / \; \sum_{x \in X} (\mathbf{Pr}[x])$$

$$= \mathbf{Pr}[x]$$

Key Randomness in One-Time Pad

- One-Time Pad uses a very long key, what if the key is not chosen randomly, instead, texts from, e.g., a book is used.
  - this is not One-Time Pad anymore
  - this does not have perfect secrecy
  - this can be broken easily

- The key in One-Time Pad should never be reused.

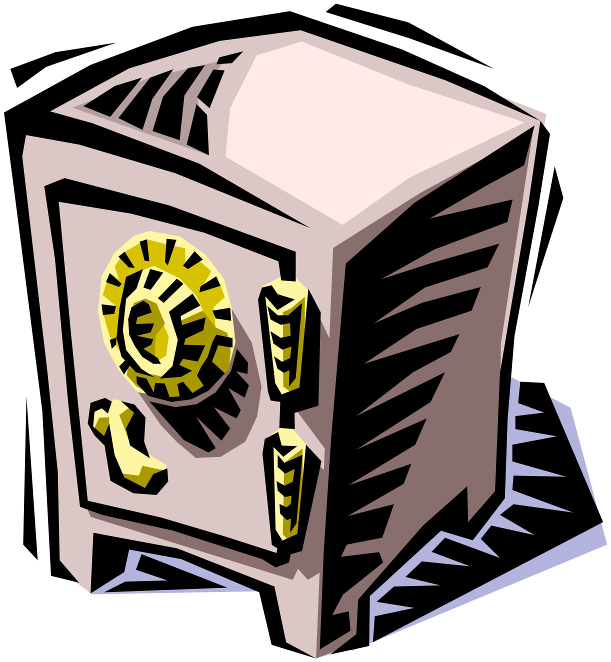
Cryptanalysis of One-Time Pad

- Provides perfect secrecy
- Disadvantages:
  - The size of key must be at least the size of the message
  - Each key is used only once. Otherwise, vulnerable to know plaintext attack. **How?**

- $X \oplus K = Y$
- The attacker knows X and Y, can compute K by using an exclusive-or operation.

Modern Cryptography

- One-time pad requires the length of the key to be the length of the plaintext and the key to be used only once. Difficult to manage.
- Alternative: design cryptosystems, where a key is used more than once.
- What about the attacker? Resource constrained, make it infeasible for adversary to break the cipher.



Spurious Keys

- Attacker can rule out certain keys, but there is a set of possible keys, out of which only one is correct.
- Spurious keys: possible, but incorrect keys.
- If the number of spurious keys is very small (or 0), the cipher is easier to break.
- Goal: bound the number of spurious keys.

Entropy

- It measures the amount of information.
- It represents the minimum number of bits required to encode all possible meanings of a message, given that all messages are equally probable.

$$H(X) = -\sum_{x \in X} P[x]\log_2 P[x]$$

Example

X is a random variable that models a message that can have four different values: x1, x2, x3, x4 that occur with probabilities 1/2, 1/4,1/8,1/8. What is the entropy H(X)?

Solution:

$H(X) = -1/2 \log_2(1/2) - 1/4 \log_2(1/4) - 2*1/8 \log_2(1/8) = 1/2 + 1/2 + 3/4 = 7/4$

Conditional Entropy

Definition

Let X and Y be two random variables. We define the conditional entropy H(X|Y) as

$$H(X\mid Y) = -\sum_{y}\sum_{x} P[y]P[x\mid y]\log_2 P[x\mid y]$$

The conditional entropy measures the average amount of information about X that is revealed by Y.

Entropy

Theorem

Given two random variables X and Y, we have

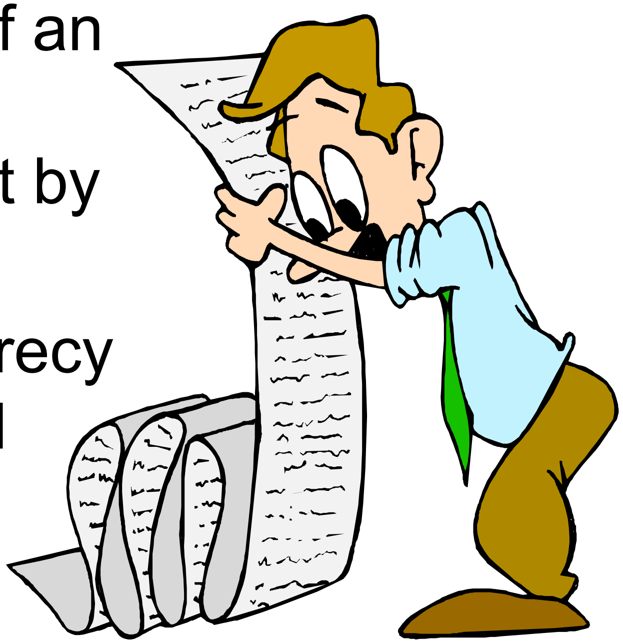
$$H(X,Y) = H(Y) + H(X|Y)$$

Corollary

H(X|Y) □ H(X) with equality if and only if X and Y are independent.

Summary

- Entropy measures the amount of information.
- A cipher has perfect secrecy if an attacker can not obtain any information about the plaintext by just observing the ciphertext.
- One time pad has perfect secrecy is the key is random and used only once.



Next Lecture…

- Symmetric cryptography
- DES
- Cryptanalysis of DES
- Modes of operation

Chapter 3.1, 3.2, 3.3, 3.4 from Stinson
Chapter 3 from Stallings
NIST FIPS for encryption modes.