Cristina Nita-Rotaru

CS355: Cryptography

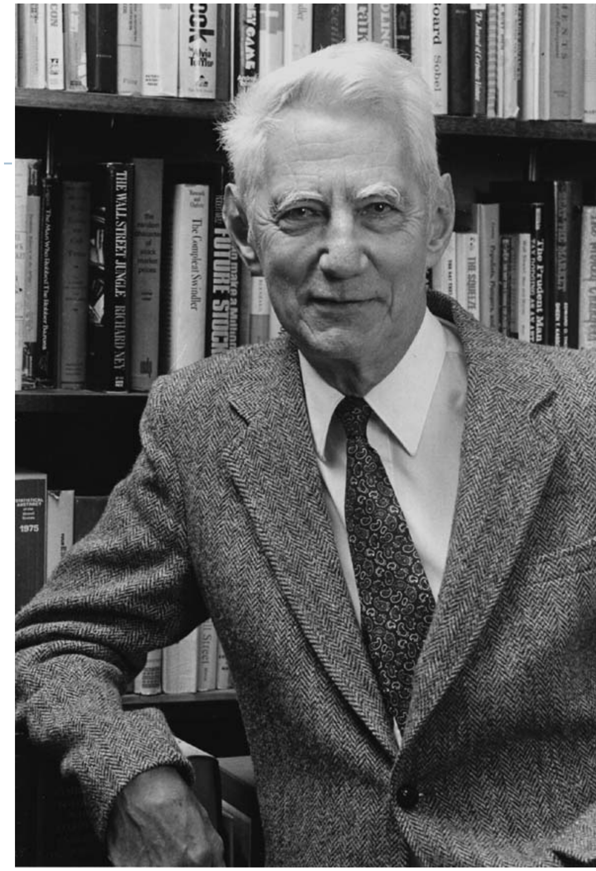
Lecture 5: One–time pad.

One-time pad

- Extend Vigenère cipher so that the key is as long as the plaintext
  - No repeat, cannot be broken by finding key length + frequency analysis
- Key is a random string that is at least as long as the plaintext
- Encryption is similar to Vigenère

History of One-time pad

- 1882 - First described by Frank Miller
- 1917 - Re-invented by Gilbert Vernam; one time pad also known as the Vernam cipher
- 1919 - Patented by Vernam
- Joseph Mauborgne recognized that having the key totally random increased security
- 1949 – showed the One-time pad had perfect secrecy, Shannon



Gilbert Sandford Vernam (1890 - 1960), was AT&T Bell Labs engineer

Joseph Mauborgne (1881-1971) was a Major General in the United States Army

Claude Elwood Shannon (1916 - 2001), American electronic engineer and mathematician, was "the father of information theory

One-time pad: encryption and decryption

Key is chosen randomly

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

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

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

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

$d_k(Y) = (y_1- k_1\ \ y_2-k_2\ \ldots\ y_n-k_n) \bmod m$

Binary version of One-time pad

Plaintext space = Ciphtertext space =

Keyspace = $\{0,1\}^n$

Key is chosen randomly

For example:

- Plaintext is 11011011
- Key is 01101001
- Then ciphertext is 10110010

Bit operators

- Bit AND

  $0 \wedge 0 = 0$ $0 \wedge 1 = 0$ $1 \wedge 0 = 0$ $1 \wedge 1 = 1$

- Bit OR

  $0 \vee 0 = 0$ $0 \vee 1 = 1$ $1 \vee 0 = 1$ $1 \vee 1 = 1$

- Addition mod 2 (also known as Bit XOR)

  $0 \oplus 0 = 0$ $0 \oplus 1 = 1$ $1 \oplus 0 = 1$ $1 \oplus 1 = 0$

Security of One-time pad

- Intuitively, it is secure …
- The key is random, so the ciphertext is completely random

Information-theoretic security

- Basic Idea: Ciphertext should provide no "information" about plaintext
- We also say such a scheme has perfect secrecy.
- One-time pad has perfect secrecy
  - E.g., suppose that the ciphertext is "Hello", can we say any plaintext is more likely than another plaintext?
- Result due to Shannon, 1949

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

- The key in One-Time Pad should never be reused.
  - If it is reused, it is insecure!

Limitations of One-time pad

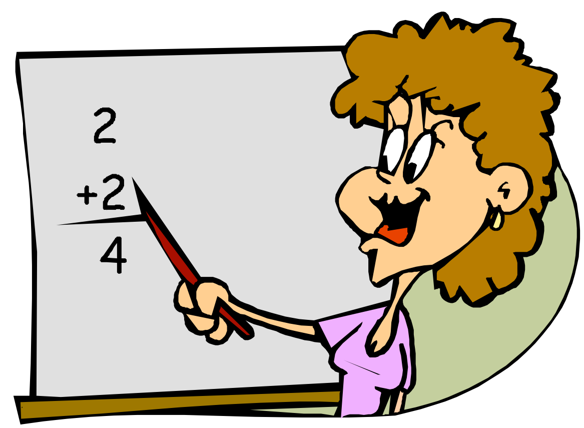
- Perfect secrecy $\Rightarrow$ key-length $\geq$ msg-length
- Difficult to use in practice

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.

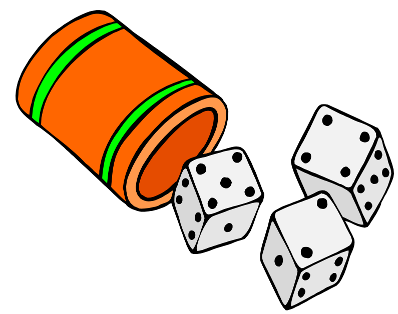
  C. E. Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal, vol.28-4, pp 656--715, 1949.

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) $0 \leq Pr(A) \leq 1$ for any set $\boldsymbol{A}$ ***in*** $\boldsymbol{S}$.
(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 $Ei \cap Ej = 0$, for all $\boldsymbol{i \neq j}$ then:

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

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)

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

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

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

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 $x \in X$ and all $y \in Y$.

Bayes' theorem

Find the conditional probability of event X given the conditional probability of event Y and the unconditional probabilities of events X and Y.

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 $x \in X$ and all $y \in Y$.

End math

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: {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};

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

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

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

P = plaintext

C = ciphertext

K = key

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 $x \in P$ and $y \in C$**, where P is the set of plaintext and C is the set of ciphertext.

What can I say about Pr[x|y] and Pr[x], for all x ∈ P and y ∈ C,

Bayes:

given

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

Don't know it, but can be computed

Don't know it, but can be computed

KNOWN, Pr[x], Pr[k]

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

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

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

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

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 HAVE PERFECT SECRECY?

One-time pad has perfect secrecy

- $P = C = K = \{0,1\}^n$, key is chosen randomly, key used once per message

Proof: We need to show that for any probability of the plaintext, $\forall x\ \forall y$, $\mathbf{Pr}\,[x \mid y] = \mathbf{Pr}[x]$

$$\mathbf{Pr}\,[x \mid y] = \mathbf{Pr}[x]\,\mathbf{Pr}\,[y \mid x] \,/\, \mathbf{Pr}[y] \text{ (Bayes)}$$

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

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

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

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

Take home lessons

- One-time pad difficult to use in practice
  - Key must be random
  - As long as the message
  - Used only once
- Perfect secrecy, theoretical model for security
- One time pad has perfect secrecy