Shannon's Theory

Dr. Odelu Vanga

Computer Science and Engineering
Indian Institute of Information Technology Sri City

odelu.vanga@iiits.in

Feb. 02, 2021

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.
2. A particular key $k \in \mathcal{K}$ is used for only one encryption.

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.
2. A particular key $k \in \mathcal{K}$ is used for only one encryption.
3. Plaintext $\mathcal{P}$ defines a r.v. denoted by X, and a priory probability that plaintext occurs denoted by $Pr[X = x]$.

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.
2. A particular key $k \in \mathcal{K}$ is used for only one encryption.
3. Plaintext $\mathcal{P}$ defines a r.v. denoted by X, and a priory probability that plaintext occurs denoted by $Pr[X = x]$.
4. The key chosen with some fixed probability distribution, so key also defines a r.v., denoted by K. Denote the probability that key K is chosen by $pr[K = k]$.

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.
2. A particular key $k \in \mathcal{K}$ is used for only one encryption.
3. Plaintext $\mathcal{P}$ defines a r.v. denoted by X, and a priory probability that plaintext occurs denoted by $Pr[X = x]$.
4. The key chosen with some fixed probability distribution, so key also defines a r.v., denoted by K. Denote the probability that key K is chosen by $pr[K = k]$.
5. The probability distributions on $\mathcal{P}$ and $\mathcal{K}$ induce a probability distribution on $\mathcal{C}$. So, ciphertext also a r.v., denoted by Y.

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.
2. A particular key $k \in \mathcal{K}$ is used for only one encryption.
3. Plaintext $\mathcal{P}$ defines a r.v. denoted by X, and a priory probability that plaintext occurs denoted by $Pr[X = x]$.
4. The key chosen with some fixed probability distribution, so key also defines a r.v., denoted by K. Denote the probability that key K is chosen by $pr[K = k]$.
5. The probability distributions on $\mathcal{P}$ and $\mathcal{K}$ induce a probability distribution on $\mathcal{C}$. So, ciphertext also a r.v., denoted by Y.

Note that key is chosen before the plaintext knows, so that plaintext and key are independent r.v.'s.

Perfect Secrecy

- For a key $k \in \mathcal{K}$, we define

$$C(k) = \{E_k(x) : x \in \mathcal{P}\}$$

The set of all possible ciphertexts if k is the key

Perfect Secrecy

- For a key $k \in \mathcal{K}$, we define

$$C(k) = \{E_k(x) : x \in \mathcal{P}\}$$

  The set of all possible ciphertexts if k is the key

- For every $y \in \mathcal{C}$, we have

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

  Note $x = D_k(E_k(x)) = D_k(y)$

Perfect Secrecy

- For a key $k \in \mathcal{K}$, we define

$$C(k) = \{E_k(x) : x \in \mathcal{P}\}$$

The set of all possible ciphertexts if k is the key

- For every $y \in \mathcal{C}$, we have

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

Note $x = D_k(E_k(x)) = D_k(y)$

- For $y \in \mathcal{C}$ and $x \in \mathcal{P}$, we have

$$Pr[Y = y | X = x] = \sum_{\{k : x = D_k(y)\}} Pr[K = k]$$

Bayes' Theorem

$$Pr[X = x|Y = y] = \frac{Pr[X = x] \sum_{\{k:x=D_k(y)\}} Pr[K = k]}{\sum_{\{k:y \in C(k)\}} Pr[K = k]Pr[X = D_k(y)]}$$

Bayes' Theorem

$$Pr[X = x|Y = y] = \frac{Pr[X = x] \sum_{\{k: x = D_k(y)\}} Pr[K = k]}{\sum_{\{k: y \in C(k)\}} Pr[K = k] Pr[X = D_k(y)]}$$

Example

Let $\mathcal{P} = \{a, b\}$ with $Pr[a] = 1/4$, $Pr[b] = 3/4$
$\mathcal{K} = \{k_1, k_2, k_3\}$ with $Pr[k_1] = 1/2$, $Pr[k_2] = Pr[k_3] = 1/4$,
and $\mathcal{C} = \{1, 2, 3, 4\}$.
Suppose encryption rule is defined as

$E_k(x)$	a	b
k_1	1	2
k_2	2	3
k_3	3	4

Find the probability $Pr[X = x|Y = y]$

Perfect Secrecy

Definition

A cryptosystem has perfect secrecy if

$$Pr[X = x | Y = y] = Pr[X = x]$$

for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.

Perfect Secrecy

Definition

A cryptosystem has perfect secrecy if

$$Pr[X = x | Y = y] = Pr[X = x]$$

for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.

Theorem

Suppose the 26 keys in the Shift Cipher are used with equal probability $1/26$. Then for any plaintext probability distribution, the Shift Cipher has perfect secrecy

Perfect Secrecy

Definition

A cryptosystem has perfect secrecy if

$$Pr[X = x|Y = y] = Pr[X = x]$$

for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.

Theorem

Suppose the 26 keys in the Shift Cipher are used with equal probability $1/26$. Then for any plaintext probability distribution, the Shift Cipher has perfect secrecy

We have, $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26}$, and define encryption rule as

$$y = E_k(x) = (x + k) \pmod{26}$$

where $x \in \mathcal{P}$ and $k \in \mathcal{K}$.

Perfect Secrecy

10/09/2019

Theorem

Suppose $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *is a cryptosystem, where* $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$.

Then
the cryptosystem provides perfect secrecy

if and only if

Perfect Secrecy

10/09/2019

Theorem

Suppose $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *is a cryptosystem, where* $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$.

Then
the cryptosystem provides perfect secrecy

if and only if

- *every key is used with equal probability* $1/|\mathcal{K}|$, *and*

Perfect Secrecy

10/09/2019

Theorem

Suppose $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *is a cryptosystem, where* $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$.

Then
the cryptosystem provides perfect secrecy

if and only if

- *every key is used with equal probability* $1/|\mathcal{K}|$, *and*
- *for every* $x \in \mathcal{P}$ *and for every* $y \in \mathcal{C}$, *there is a unique key* k *such that* $E_k(x) = y$

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy

For each $x \in \mathcal{P}$ and $y \in \mathcal{C}$,

there must be at least one key k such that $E_k(x) = y$.

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy
For each $x \in \mathcal{P}$ and $y \in \mathcal{C}$,
there must be at least one key k such that $E_k(x) = y$.
So, we have the inequalities

$$|\mathcal{C}| = |\{E_k(x) : k \in \mathcal{K}\}| \leq |\mathcal{K}|$$

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy

For each $x \in \mathcal{P}$ and $y \in \mathcal{C}$,

there must be at least one key k such that $E_k(x) = y$.

So, we have the inequalities

$$|\mathcal{C}| = |\{E_k(x) : k \in \mathcal{K}\}| \leq |\mathcal{K}|$$

But, we assume that $|\mathcal{C}| = |\mathcal{K}|$.

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy
For each $x \in \mathcal{P}$ and $y \in \mathcal{C}$,
there must be at least one key k such that $E_k(x) = y$.
So, we have the inequalities

$$|\mathcal{C}| = |\{E_k(x) : k \in \mathcal{K}\}| \leq |\mathcal{K}|$$

But, we assume that $|\mathcal{C}| = |\mathcal{K}|$.
Hence, it must be the case that

$$|\{E_k(x) : k \in \mathcal{K}\}| = |\mathcal{K}|$$

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy
For each $x \in \mathcal{P}$ and $y \in \mathcal{C}$,
there must be at least one key k such that $E_k(x) = y$.
So, we have the inequalities

$$|\mathcal{C}| = |\{E_k(x) : k \in \mathcal{K}\}| \leq |\mathcal{K}|$$

But, we assume that $|\mathcal{C}| = |\mathcal{K}|$.
Hence, it must be the case that

$$|\{E_k(x) : k \in \mathcal{K}\}| = |\mathcal{K}|$$

That is, there do not exist two distinct keys k_1 and k_2 such that $E_{k_1}(x) = E_{k_2}(x) = y$.

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy
For each $x \in \mathcal{P}$ and $y \in \mathcal{C}$,
there must be at least one key k such that $E_k(x) = y$.
So, we have the inequalities

$$|\mathcal{C}| = |\{E_k(x) : k \in \mathcal{K}\}| \leq |\mathcal{K}|$$

But, we assume that $|\mathcal{C}| = |\mathcal{K}|$.
Hence, it must be the case that

$$|\{E_k(x) : k \in \mathcal{K}\}| = |\mathcal{K}|$$

That is, there do not exist two distinct keys k_1 and k_2 such that $E_{k_1}(x) = E_{k_2}(x) = y$.
Hence, we have shown that for any $x \in \mathcal{P}$ and $y \in \mathcal{C}$, there is exactly one key k such that $E_k(x) = y$. □

Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.

Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.

Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.
Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.
Suppose the keys are $k_1, k_2, \ldots, k_n$, such that $E_{k_i}(x_i) = y$, $1 \leq i \leq n$.

Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.
Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.
Suppose the keys are $k_1, k_2, \ldots, k_n$, such that $E_{k_i}(x_i) = y$, $1 \leq i \leq n$.
Using Bayes' theorem, we have

$$Pr[x_i|y] = \frac{Pr[y|x_i]Pr[x_i]}{Pr[y]} = \frac{Pr[k_i]Pr[x_i]}{Pr[y]}$$

Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.
Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.
Suppose the keys are $k_1, k_2, \ldots, k_n$, such that $E_{k_i}(x_i) = y$, $1 \leq i \leq n$.
Using Bayes' theorem, we have

$$Pr[x_i|y] = \frac{Pr[y|x_i]Pr[x_i]}{Pr[y]} = \frac{Pr[k_i]Pr[x_i]}{Pr[y]}$$

- Consider the perfect secrecy condition $Pr[x_i|y] = Pr[x_i]$.

Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.
Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.
Suppose the keys are $k_1, k_2, \ldots, k_n$, such that $E_{k_i}(x_i) = y$, $1 \leq i \leq n$.
Using Bayes' theorem, we have

$$Pr[x_i|y] = \frac{Pr[y|x_i]Pr[x_i]}{Pr[y]} = \frac{Pr[k_i]Pr[x_i]}{Pr[y]}$$

- Consider the perfect secrecy condition $Pr[x_i|y] = Pr[x_i]$.
- This implies that, $Pr[k_i] = Pr[y]$, for $1 \leq i \leq n$.

Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.
Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.
Suppose the keys are $k_1, k_2, \ldots, k_n$, such that $E_{k_i}(x_i) = y$, $1 \leq i \leq n$.
Using Bayes' theorem, we have

$$Pr[x_i|y] = \frac{Pr[y|x_i]Pr[x_i]}{Pr[y]} = \frac{Pr[k_i]Pr[x_i]}{Pr[y]}$$

- Consider the perfect secrecy condition $Pr[x_i|y] = Pr[x_i]$.
- This implies that, $Pr[k_i] = Pr[y]$, for $1 \leq i \leq n$.
- This says that all keys are used with equal probability (namely, $Pr[y]$).

Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.
Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.
Suppose the keys are $k_1, k_2, \ldots, k_n$, such that $E_{k_i}(x_i) = y$, $1 \leq i \leq n$.
Using Bayes' theorem, we have

$$Pr[x_i|y] = \frac{Pr[y|x_i]Pr[x_i]}{Pr[y]} = \frac{Pr[k_i]Pr[x_i]}{Pr[y]}$$

- Consider the perfect secrecy condition $Pr[x_i|y] = Pr[x_i]$.
- This implies that, $Pr[k_i] = Pr[y]$, for $1 \leq i \leq n$.
- This says that all keys are used with equal probability (namely, $Pr[y]$).
- Since the number of keys are $|\mathcal{K}|$, we must have that $Pr[k] = 1/|\mathcal{K}|$, for $k \in \mathcal{K}$.

Perfect Secrecy

Could you prove the converse of the theorem ?

Continue.....

Given

- every key is used with equal probability $1/|\mathcal{K}|$, and
- for every $x \in \mathcal{P}$ and for every $y \in \mathcal{C}$, there is a unique key k such that $E_k(x) = y$

Prove the cryptosystem provides perfect secrecy. $\square$

Bayes' theorem:

$$Pr[X = x|Y = y] = \frac{Pr[X = x] \sum_{\{k:x=D_k(y)\}} Pr[K = k]}{\sum_{\{k:y \in C(k)\}} Pr[K = k] Pr[X = D_k(y)]}$$

Latin Square

Let n be a positive integer. A Latin square of order n is an $n \times n$ array L of the integers $1, \ldots, n$ such that every one of the n integers occurs exactly once in each row and each column of L.

Latin Square

Let n be a positive integer. A Latin square of order n is an $n \times n$ array L of the integers $1, \ldots, n$ such that every one of the n integers occurs exactly once in each row and each column of L.

An example of a Latin square of order 3 is as follows:

1	2	3
3	1	2
2	3	1

Latin Square

Let n be a positive integer. A Latin square of order n is an $n \times n$ array L of the integers $1, \ldots, n$ such that every one of the n integers occurs exactly once in each row and each column of L.

An example of a Latin square of order 3 is as follows:

1	2	3
3	1	2
2	3	1

Given any Latin square L of order n, we can define a related cryptosystem. Take $\mathcal{P} = \mathcal{C} = \mathcal{K}$. For $1 \leq i \leq n$, the encryption rule defined as

$$E_i(j) = L(i, j)$$

(Hence each row of L gives rise to one encryption rule.)

Latin Square

Let n be a positive integer. A Latin square of order n is an $n \times n$ array L of the integers $1, \ldots, n$ such that every one of the n integers occurs exactly once in each row and each column of L.

An example of a Latin square of order 3 is as follows:

1	2	3
3	1	2
2	3	1

Given any Latin square L of order n, we can define a related cryptosystem. Take $\mathcal{P} = \mathcal{C} = \mathcal{K}$. For $1 \leq i \leq n$, the encryption rule defined as

$$E_i(j) = L(i, j)$$

(Hence each row of L gives rise to one encryption rule.)

Give a complete proof that this Latin square cryptosystem achieves perfect secrecy provided that every key is used with equal probability.

One-Time Pad

- One well-known realization of perfect secrecy is the Vernam One-time Pad.
- First described by Gilbert Vernam in 1917 for use in automatic encryption and decryption of telegraph messages.
- One-time Pad was thought for many years to be an "unbreakable" cryptosystem.
- But, there was no proof of this until Shannon developed the concept of perfect secrecy over 30 years later.

One-Time Pad

Definition (One-Time Pad)

Let $n \geq 1$ be an integer, and take $\mathcal{P} = \mathcal{C} = \mathcal{K} = (Z_2)^n$. If
$k = (k_1, k_2, \ldots, k_n)$ in $\mathcal{K}$,
$x = (x_1, x_2, \ldots, x_n)$ in $\mathcal{P}$, and
$y = (y_1, y_2 \ldots, y_n)$ in $\mathcal{C}$,
we define

One-Time Pad

Definition (One-Time Pad)

Let $n \geq 1$ be an integer, and take $\mathcal{P} = \mathcal{C} = \mathcal{K} = (Z_2)^n$. If
$k = (k_1, k_2, \ldots, k_n)$ in $\mathcal{K}$,
$x = (x_1, x_2, \ldots, x_n)$ in $\mathcal{P}$, and
$y = (y_1, y_2 \ldots, y_n)$ in $\mathcal{C}$,
we define

$$E_k(x) = (x_1 + k_1, x_2 + k_2, \ldots, x_n + k_n) \pmod 2$$

$$D_k(y) = (y_1 + k_1, y_2 + k_2, \ldots, y_n + k_n) \pmod 2$$

Decryption is also identical to the encryption.

One-Time Pad

Definition (One-Time Pad)

Let $n \geq 1$ be an integer, and take $\mathcal{P} = \mathcal{C} = \mathcal{K} = (Z_2)^n$. If
$k = (k_1, k_2, \ldots, k_n)$ in $\mathcal{K}$,
$x = (x_1, x_2, \ldots, x_n)$ in $\mathcal{P}$, and
$y = (y_1, y_2 \ldots, y_n)$ in $\mathcal{C}$,
we define

$$E_k(x) = (x_1 + k_1, x_2 + k_2, \ldots, x_n + k_n) \pmod 2$$

$$D_k(y) = (y_1 + k_1, y_2 + k_2, \ldots, y_n + k_n) \pmod 2$$

Decryption is also identical to the encryption.

Note that $\pmod 2$ is equivalent to the exclusive-or ($\oplus$).

One-Time Pad - Drawbacks

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13

plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25

plaintext (m)	,	.	:	;	space	’
Assigned No.	26	27	28	29	30	31

Assume 5-bit character representation

One-Time Pad - Drawbacks

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13

plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25

plaintext (m)	,	.	:	;	space	’
Assigned No.	26	27	28	29	30	31

Assume 5-bit character representation

Example (One key for one encryption)

Generate a ciphertext with random key given by *I am good* for the message *it’s true* using the above character encoding.

One-Time Pad - Perfect Secrecy

Definition

A cipher (E, D) over $(\mathcal{K}, \mathcal{P}, \mathcal{C})$ has perfect secrecy if $\forall x_0, x_1 \in \mathcal{P}$, $(|x_0| = |x_1|)$ and $\forall y \in \mathcal{C}$

$$Pr[E_k(x_0) = y] = Pr[E_k(x_1) = y]$$

where $k \leftarrow_R \mathcal{K}$.

One-Time Pad - Perfect Secrecy

Definition

A cipher (E, D) over $(\mathcal{K}, \mathcal{P}, \mathcal{C})$ has perfect secrecy if $\forall x_0, x_1 \in \mathcal{P}$, $(|x_0| = |x_1|)$ and $\forall y \in \mathcal{C}$

$$Pr[E_k(x_0) = y] = Pr[E_k(x_1) = y]$$

where $k \leftarrow_R \mathcal{K}$.

Theorem

The one-time pad encryption scheme is perfectly secure.

One-Time Pad - Perfect Secrecy

Definition

A cipher (E, D) over $(\mathcal{K}, \mathcal{P}, \mathcal{C})$ has perfect secrecy if $\forall x_0, x_1 \in \mathcal{P}$, $(|x_0| = |x_1|)$ and $\forall y \in \mathcal{C}$

$$Pr[E_k(x_0) = y] = Pr[E_k(x_1) = y]$$

where $k \leftarrow_R \mathcal{K}$.

Theorem

The one-time pad encryption scheme is perfectly secure.

Proof(One-time pad : perfect secrecy).

We have to show $\forall x_0, x_1 \in \mathcal{P}$, $(|x_0| = |x_1|)$ and $\forall y \in \mathcal{C}$

$$Pr[E_k(x_0) = y] = Pr[E_k(x_1) = y]$$

□

One-Time Pad - Drawbacks

- Vernam patented his idea in the hope that it would have widespread commercial use.
- The fact that $|\mathcal{K}| \geq |\mathcal{P}|$, means that the amount of key that must be communicated securely is at least as big as the amount of plaintext.
- This would not be a major problem if the same key could be used to encrypt different messages; however, the security of unconditionally secure cryptosystems depends on the fact that each key is used for only one encryption.

One-Time Pad - Drawbacks

- Vernam patented his idea in the hope that it would have widespread commercial use.
- The fact that $|\mathcal{K}| \geq |\mathcal{P}|$, means that the amount of key that must be communicated securely is at least as big as the amount of plaintext.
- This would not be a major problem if the same key could be used to encrypt different messages; however, the security of unconditionally secure cryptosystems depends on the fact that each key is used for only one encryption.
- The One-time Pad is vulnerable to a known-plaintext attack