Computer Science 418

Classical Ciphers and Perfect Security

Mike Jacobson

Department of Computer Science
University of Calgary

Week 2

Outline

Recreational Reading

For cryptography in history and literature, Simon Singh's *The Code Book* (Doubleday 1999) is highly recommended. See also Singh's website `www.simonsingh.net`.

The most comprehensive source on cryptography in military history is David Kahn's *The Code Breakers* (1967).

Classical Ciphers

Classical ciphers are usually belong to one of the following two types: substitution or transposition ciphers.

Definition 1 (Substitution cipher)

A cipher for which encryption replaces each plaintext symbol by some ciphertext symbol without changing the order of the plaintext symbols.

Definition 2 (Transposition cipher)

A cipher in which the ciphertext is a rearrangement (*i.e.* permutation) of the plaintext symbols.

Modern Usage

It turns out that individually, substitution ciphers and transposition ciphers are generally insecure.

However, when alternating them repeatedly,

$$M \longrightarrow \boxed{\text{T}} \longrightarrow \boxed{\text{S}} \longrightarrow \boxed{\text{T}} \longrightarrow \boxed{\text{S}} \longrightarrow \cdots \longrightarrow \boxed{\text{T}} \longrightarrow \boxed{\text{S}} \longrightarrow C \ ,$$

they become very secure.

This is how modern symmetric cryptosystems are designed.

Monoalphabetic Substitution Ciphers

Substitution ciphers come in two types:

- monoalphabetic (one cipher alphabet)
- polyalphabetic (multiple cipher alphabets)

Definition 3 (Monoalphabetic Substitution cipher)

A substitution cipher that uses a single ciphertext alphabet.

Example: Shift Cipher

Encrypt and decrypt a shift cipher with a *Vigènere tableau*

Encryption: The key (shift) represents a column. The ciphertext letter is located at the intersection of this column and the row given by the corresponding plaintext letter.

- Eg. to encrypt the letter 'i' with a Caesar cipher (key letter D), look up the row for 'i' and the column for 'D' in the Vigenère tableau. The entry in the tableau gives the ciphertext letter, in this case 'L'.

Decryption: Look up a ciphertext letter in the column given by the key. The corresponding plaintext letter is located at the beginning of that row.

- Eg. to decrypt 'L' under key 'D', find the entry for L in the column for D. The corresponding row begins with 'i' which which is the plaintext letter.

The Vigenére Tableau

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Substitution Ciphers in Literature

Fiction literature is full of examples of monoalphabetic substitution ciphers:

- Edgar Allan Poe's *The Gold Bug*
- Sir Arthur Conan Doyle's *The Adventure of the Dancing Men* (a Sherlock Holmes story)
- Even the bible contains examples, derived from a cipher called *atbash*

Security of Monoalphabetic Substitution Ciphers

Substitution ciphers are in general completely insecure:

1. Highly vulnerable to KPA's. Each portion of corresponding plaintext and ciphertext reveals some of the cipher.
   - Eg. For shift ciphers, one corresponding plaintext-ciphertext pair actually reveals the key!
2. Each plaintext letter is encrypted to the same ciphertext letter.
   - Thus, frequent ciphertext letters correspond to common plaintext letters (*e.g.* "e" in English).
   - Also pairs of identical ciphertext letters correspond to such paintext letter pairs (*e.g.* "XX" corresponds to "yy")

Security, cont.

3. Redundancy in any language generally yields the key, given a sufficient amount of ciphertext (COA).
   - frequency distribution of the plaintext alphabet (letters, pairs of letters, triples of letters etc.) in a given language can be established statistically and compared with the ciphertext (see frequency and digraph handouts).
   - The method is called the *phi-statistic*. The concept of redundancy can be mathematically formalized.

Of course this assumes "normal" text.

Example 4

A pathological example of how frequency analysis can sometimes lead us astray: *Gadsby*, by Ernest Vincent Wright. This 50,000 word novel is written entirely without using the letter *E*.

Codes

Definition 5 (Code)

A technique by which words or letter combinations are replaced by a set of predetermined codewords.

Codes are essentially monoalphabetic substitution ciphers with very large plaintext alphabets.

Historical examples:

- Mary Queen of Scotts conspiring to overthrow Queen Elizabeth I and gain the English throne
- Famous 1917 WW I Zimmerman telegram
- Navajo Code talkers in WW II

Polyalphabetical Substitution Ciphers

Definition 6 (polyalphabetic substitution cipher)

A substitution cipher in which several cipher alphabets are used in the replacement of the plaintext characters.

Example 7

The Vigenère Cipher: Originally described by Giovan Batista Belaso (1553) in *La cifra del. Sig. Giovan Batista Belaso*. Rediscovered many times. To the French, it became known as *le chiffre indéchiffrable* ('the unbreakable cipher'). It is basically a collection of shift ciphers, each corresponding to a letter in a key word.

Vigenère Example

Plaintext: `stay in current position`

Key: `BLACKSTONE`

Encryption: again done easiest via a Vigenère tableau, except now we need to consider multiple columns.

- To encrypt the first letter ('s'), look up the row for 's' and the column for 'B' in the Vigenère tableau. The entry in the tableau gives the ciphertext letter, in this case 'T'.
- To encrypt the second letter ('t'), find the intersection of the row given by plaintext letter 't' with the column given by key letter 'L' to obtain the ciphertext letter 'E'.

Ciphertext: `TEAAS FVIEV FYTRY KBHVS OXAUS`

Vigenére Example, cont.

Note: The ciphertext is written in groups of 5 letters to obscure spacing.

- If the number of characters is not a multiple of 5, we append *nulls* (bogus characters).
- can apply to any substitution cipher

Note: This is a polyalphabetic substitution cipher. The number of cipher alphabets is equal to the number of letters in the key word (10 in the example).

Cryptanalysis of the Vigenère Cipher

First, determine the number n of cipher alphabets (length of the key word) using methods like the *kappa text* or *Kasiski's factoring method*

Once n is known, consider for $1 \leq i \leq n$ the i-th subtext considering of the ciphertext letters in positions $i, i+n, i+2n, i+3n, \ldots$.

- Each of these is simply text encrypted with a shift cipher whose key is the i-th letter in the Vigeneère key word
- Cryptanalyze each just like any shift cipher (with frequency analysis).

Other Polyalphabetic Substitution Ciphers

Beauford cipher – slight variant of Vigenère

Mixed Vigenère – works with a Vigenère tableau in which the columns are scrambled according to some key word.

- Harder to cryptanalyze than ordinary Vigenère – need to use a technique called *symmetry of position* (see handout) to find out the column permutation – but still insecure.

Coherent Running Key cipher – like a Vigenère cipher but with a "running" *i.e.* very long) key, usually taken from a readily available text.

- Still falls to frequency analysis due to language redundancy. However, it has been proven that multiple encryption using four different running keys produces a statistically secure cipher.

Transposition Ciphers

Recall that a transposition cipher is a rearrangement (permutation) of the plaintext letters.

Definition 8 (Route cipher)

A transposition cipher where the plaintext is arranged in some geometric figure and the ciphertext is obtained by rearranging the plaintext according to some route through the figure.

Definition 9 (Columnar Transposition)

The message is arranged horizontally in a rectangle. The key is used to generate a permutation of the columns. The ciphertext is read vertically from the permuted columns.

Route Cipher Example

Plaintext: `Now is the time for all good men`

Encryption: arrange the plaintext by rows into a rectangle of K columns and extract the ciphertext by the columns.

For $K = 5$:

```
N O W I S
T H E T I
M E F O R
A L L G O
O D M E N
```

Ciphertext: `NTMAO OHELD WEFLM ITOGE SIRON`

Columnar Transposition Example

key: `SCHMID` (relative order of key letters dictates column permutation)

```
key:    S C H M I D
order:  6 1 3 5 4 2
```

plaintext: `sell all stock on Monday`

```
6  1  3  5  4  2
S  E  L  L  A  L
L  S  T  O  C  K
O  N  M  O  N  D
A  Y
```

ciphertext (read columnwise in given order): `ESNYL KDLTM ACNLO OSLOA`

Decryption: Write ciphertext in columns in the correct order (and shape) of the rectangle (dictated by ciphertext length and key length).

Note that we can't use nulls at the end of the ciphertext.

Cryptanalysis of Columnar Transposition

Vulnerable to a COA:

- Guess the dimensions of the rectangle
- Determine the order of the columns via frequency counts (which will be the same as for English text). Place columns adjacent to each other if they produce common latter pairs (*e.g.* QX is extremely unlikely, but EN is highly likely).

Information Theory

Claude Shannon is widely hailed as the "father of information theory".

- seminal work in the late 1940's and early 1950's in this field
- credited with turning cryptography into a scientific discipline.
- in addition, modern satellite transmission would not be possible without his work

Information theory measures the amount of information conveyed by a piece of data.

- captures how much partial information you need to have in order to obtain full information.

Partial Information

For example, partial information reveals the full word or phrase in:

- Abbreviations — "LOL"
- Contractions — "I've"
- Omitted vowels — "BSKTBLL"
- Glyphs — smiley face

How much partial information is enough? E.g. "BLL" could mean "ball", "bell", "bill", "bull", ...

Definitions

Definition 10

Sample space – a finite set $\mathcal{X} = \{X_1, X_2, \ldots, X_n\}$ whose elements are called *outcomes*

Probability distribution on $\mathcal{X}$ – a complete set of probabilities; *i.e.*

$$p(X_1), p(X_2), \ldots, p(X_n) \geq 0 \quad \text{with} \quad \sum_{i=1}^{n} p(X_i) = 1.$$

Random variable – a pair X consisting of a sample space $\mathcal{X}$ and a probability distribution on $\mathcal{X}$. The *(a priori) probability* that X takes on the value $x \in \mathcal{X}$ is denoted by $p(X = x)$ or simply $p(x)$.

Joint and Conditional Probability

Let X and Y be random variables.

Definition 11

Joint probability $p(x, y)$ – probability that $p(X = x)$ *and* $p(Y = y)$.

Conditional probability $p(x|y)$ is the probability that $p(X = x)$ *given that* $p(Y = y)$.

Joint and conditional probabilities are related as follows:

$$p(x, y) = p(x|y)p(y) \ .$$

Bayes Theorem

Theorem 1 (Bayes Theorem)

If $p(y) > 0$, *then*

$$p(x|y) = \frac{p(x)p(y|x)}{p(y)} \ .$$

Proof.

Clearly $p(x, y) = p(y, x)$, so $p(x|y)p(y) = p(y|x)p(x)$. Now divide by $p(y)$. □

Independence

Definition 12

Two random variables X, Y are *independent* if $p(x, y) = p(x)p(y)$.

Example 13

A fair coin toss is modeled by a random variable on the sample space $\mathcal{X} = \{\text{heads, tails}\}$ so that $p(\text{heads}) = p(\text{tails}) = 1/2$. Two fair coin tosses in a row represent independent events as each of the 4 possible outcomes has (joint) probability $1/4$.

Corollary 2

X *and* Y *are independent if and only of* $p(x|y) = p(x)$ *for all* $x \in \mathcal{X}, y \in \mathcal{Y}$ *with* $p(y) > 0$.

Idea of Perfect Secrecy

Recall the notion of *unconditional security* which requires that an adversary with unlimited computing power cannot defeat the system. This relates to *perfect secrecy*.

Intuitively, for perfect secrecy, ciphertexts should reveal no information whatsoever about plaintexts.

Theoretically unbreakable!

Setup

We consider the following three probability distributions:

- A random variable on the message space $\mathcal{M}$; plaintexts M occur with probabilities $p(M)$ such that $\sum_{M\in\mathcal{M}} p(M) = 1$.
- A random variable on the ciphertext space $\mathcal{C}$; ciphertexts C occur with probabilities $p(C)$ such that $\sum_{C\in\mathcal{C}} p(C) = 1$.
- A random variable on the key space $\mathcal{K}$; keys K are selected with *prior* probabilities $p(K)$ such that $\sum_{K\in\mathcal{K}} p(K) = 1$.

We assume that the random variables on $\mathcal{K}$ and $\mathcal{M}$ are independent, as keys are usually chosen before the plaintext is ever seen.

- Most of the time, each key is selected with equal likelyhood $1/|\mathcal{K}|$, regardless of the nature of the messages to be encrypted.

Notation

We consider the following probabilities:

- $p(M)$ — (a priori) probability that plaintext M is sent.
- $p(C)$ – probability that ciphertext C was received.
- $p(M|C)$ — probability that plaintext M was sent, given that ciphertext C was received.
- $p(C|M)$ – probability that ciphertext C was received, given that plaintext M was sent.
- $p(K)$ – probability that key K was chosen.

Definition

Definition 14 (Perfect Secrecy)

A cryptosystem provides *perfect secrecy* if $p(M|C) = p(M)$ for all $M \in \mathcal{M}$ and $C \in \mathcal{C}$ with $p(C) > 0$.

Formally, perfect secrecy means exactly that the random variables on $\mathcal{M}$ and $\mathcal{C}$ are independent. Informally, this implies that knowing the ciphertext C gives us no information about M.

The probabilities $p(M|C)$ and $p(M)$ are hard to quantify (we may not know anything about which plaintexts occur). Bayes' Theorem relates these quantities to $p(C|M)$ and $p(C)$, and these probabilities turn out to be easier to quantify.

Equivalent Definition

Theorem 3

A cryptosystem provides perfect secrecy if and only if $p(C|M) = p(C)$ for all $M \in \mathcal{M}, C \in \mathcal{C}$ with $p(M) > 0$ and $p(C) > 0$.

Proof.

Let $M \in \mathcal{M}$ and $C \in \mathcal{C}$ with $p(M) > 0$ and $p(C) > 0$. By Bayes' Theorem,

$$p(C|M) = \frac{p(C)p(M|C)}{p(M)} .$$

Perfect secrecy means exactly that $p(M|C) = p(M)$, which is the case if and only if $p(C|M) = p(C)$. □

Intuition

Informally, perfect secrecy means that the probability of receiving a particular ciphertext C, given that M was sent (enciphered with some key K) is the same as the probability of receiving C given that any other message M was sent (possibly enciphered under another key).

Example 15

Suppose we have 3 messages, *i.e.* $\mathcal{M} = \{M_1, M_2, M_3\}$, and 3 ciphertexts $\mathcal{C} = \{C_1, C_2, C_3\}$, and all occur with equal probabilities ($p(M_1) = p(M_2) = p(M_3) = 1/3$ and $p(C_1) = p(C_2) = p(C_3) = 1/3$).

Also, suppose that we have perfect secrecy, *i.e.* $p(M|C) = p(M) = 1/3$, so by Theorem 3, $p(C|M) = p(C) = 1/3$.

This means that C_i corresponds to M_j with equal probability for all i, j.

Illustration of the Example

Each ciphertext (C_i) could be the encryption of any of the messages with equal probability.