Cryptography

April 9, 2018

Secret Writing

Comes in Two Forms

Secret Writing

Comes in Two Forms

Steganography

Cryptography

Secret Writing

Comes in Two Forms

Steganography

- From *steganos*= "covered" and *graphien*= "to write".

Cryptography

Secret Writing

Comes in Two Forms

Steganography

- From *steganos*= "covered" and *graphien*= "to write" .
- Text is written plainly but hidden from sight.

Cryptography

Secret Writing

Comes in Two Forms

Steganography

- From *steganos*= "covered" and *graphien*= "to write".
- Text is written plainly but hidden from sight.
- The presence of a message is hidden.

Cryptography

Secret Writing

Comes in Two Forms

Steganography

- From *steganos*=“covered” and *graphien*=“to write”.
- Text is written plainly but hidden from sight.
- The presence of a message is hidden.

Cryptography

- From *kryptos*=“hidden” and *graphien*=“to write”.

Secret Writing

Comes in Two Forms

Steganography

- From *steganos*="covered" and *graphien*="to write".
- Text is written plainly but hidden from sight.
- The presence of a message is hidden.

Cryptography

- From *kryptos*="hidden" and *graphien*="to write".
- Text is scrambled to hide its meaning.

Secret Writing

Comes in Two Forms

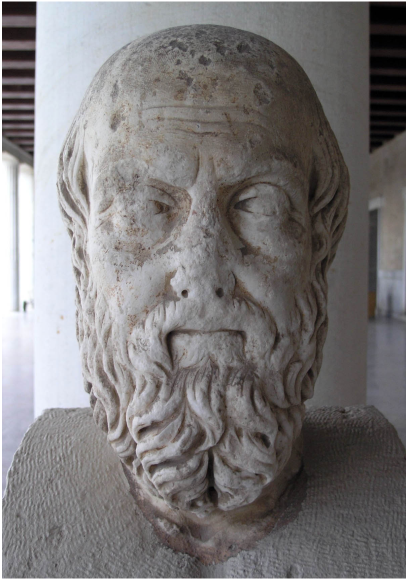
Steganography

- From *steganos*= "covered" and *graphien*= "to write".
- Text is written plainly but hidden from sight.
- The presence of a message is hidden.

Cryptography

- From *kryptos*= "hidden" and *graphien*= "to write".
- Text is scrambled to hide its meaning.
- The presence of a message is not hidden.

Herodotus



Demaratus

Recorded by the Greek historian Herodotus:

- Xerxes – husband of Esther – ruled a Persian empire that controlled much of the known world around 500 B.C.

Demaratus

Recorded by the Greek historian Herodotus:

- Xerxes – husband of Esther – ruled a Persian empire that controlled much of the known world around 500 B.C.

- Xerxes was building an army to launch a surprise attack on Athens and Sparta.

Demaratus

Recorded by the Greek historian Herodotus:

- Xerxes – husband of Esther – ruled a Persian empire that controlled much of the known world around 500 B.C.

- Xerxes was building an army to launch a surprise attack on Athens and Sparta.
- Demaratus – a Greek living in Susa – sent a message to warn the Greeks.

Demaratus

Recorded by the Greek historian Herodotus:

- Xerxes – husband of Esther – ruled a Persian empire that controlled much of the known world around 500 B.C.

- Xerxes was building an army to launch a surprise attack on Athens and Sparta.
- Demaratus – a Greek living in Susa – sent a message to warn the Greeks.
- Demaratus wrote the message on a wooden tablet which was covered with wax. The message was hidden under the wax.

Histaiaeus

Recorded by the Greek historian Herodotus:

- Histaiaeus sent a message to Aristagoras of Miletus to encourage him to revolt against Persia.

Histaiaeus

Recorded by the Greek historian Herodotus:

- Histaiaeus sent a message to Aristagoras of Miletus to encourage him to revolt against Persia.
- The head of the messenger was shaved.

Histaiaeus

Recorded by the Greek historian Herodotus:

- Histaiaeus sent a message to Aristagoras of Miletus to encourage him to revolt against Persia.
- The head of the messenger was shaved.
- The message was written on the shaved scalp.

Histaiaeus

Recorded by the Greek historian Herodotus:

- Histaiaeus sent a message to Aristagoras of Miletus to encourage him to revolt against Persia.
- The head of the messenger was shaved.
- The message was written on the shaved scalp.
- The messenger's hair was allowed to regrow before he left.

Chinese Silk

Ancient China

- Messages were written on pieces of silk.

Chinese Silk

Ancient China

- Messages were written on pieces of silk.
- The silk was balled up and covered with wax.

Chinese Silk

Ancient China

- Messages were written on pieces of silk.
- The silk was balled up and covered with wax.
- The wax ball was swallowed by a messenger.

Pliny the Elder

First Century A.D.

Described how to make invisible ink from a thithymallus plant.

Giovanni Porta

1500’s Italy:

- An ink can be made with vinegar.

Giovanni Porta

1500's Italy:

- An ink can be made with vinegar.
- Write a message on the shell of a boiled egg.

Giovanni Porta

1500's Italy:

- An ink can be made with vinegar.
- Write a message on the shell of a boiled egg.
- The ink soaks through the shell and leaves the message on the surface of the egg.

Giovanni Porta

1500's Italy:

- An ink can be made with vinegar.
- Write a message on the shell of a boiled egg.
- The ink soaks through the shell and leaves the message on the surface of the egg.
- The message can be read when the shell is removed.

Microdot

German agents in Latin America, WWII:

- Messages were photographed and shrunk to dots less than 1mm in diameter.

Microdot

German agents in Latin America, WWII:

- Messages were photographed and shrunk to dots less than 1mm in diameter.
- The film microdots were placed on top of periods in what seemed to be innocent letters.

The Weakness of Steganography

If a message is conceled only with stegonagraphy, then the message can be read as soon as it is found.

Cryptography

Message is *scrambled* to hide its **meaning**.

Cryptography

Comes in Two Forms

Cryptography

Comes in Two Forms

Transposition

Substitution

Cryptography

Comes in Two Forms

Transposition	**Substitution**
Symbols in message are re-arranged.	

Cryptography

Comes in Two Forms

Transposition

Symbols in message are re-arranged.

Substitution

Symbols in message are replaced with other symbols.

Cryptography Terminology

- **cipher**: individual letters are replaced with other symbols or letters.

Cryptography Terminology

- **cipher**: individual letters are replaced with other symbols or letters.
- **code**: words and phrases are replaced with symbols.

Cryptography Terminology

- **cipher**: individual letters are replaced with other symbols or letters.
- **code**: words and phrases are replaced with symbols.
- **plaintext**: message to be encrypted.

Cryptography Terminology

- **cipher**: individual letters are replaced with other symbols or letters.
- **code**: words and phrases are replaced with symbols.
- **plaintext**: message to be encrypted.
- **plain alphabet**: alphabet used to write plaintext (we will usually use lower-case).

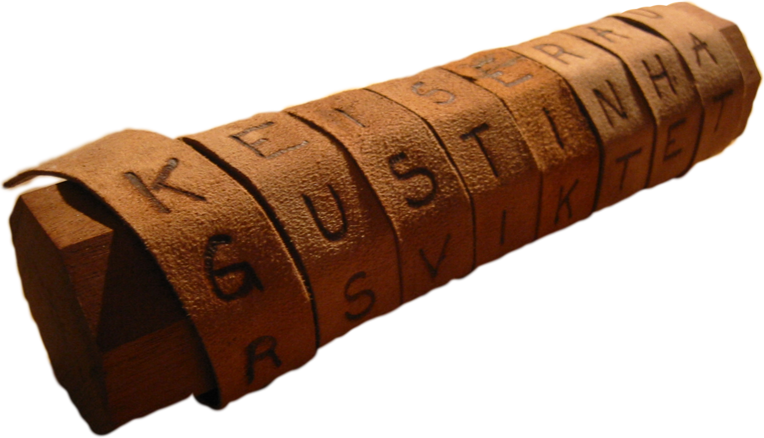
Cryptography Terminology

- **cipher**: individual letters are replaced with other symbols or letters.
- **code**: words and phrases are replaced with symbols.
- **plaintext**: message to be encrypted.
- **plain alphabet**: alphabet used to write plaintext (we will usually use lower-case).
- **ciphertext**: encrypted message.

Cryptography Terminology

- **cipher**: individual letters are replaced with other symbols or letters.
- **code**: words and phrases are replaced with symbols.
- **plaintext**: message to be encrypted.
- **plain alphabet**: alphabet used to write plaintext (we will usually use lower-case).
- **ciphertext**: encrypted message.
- **cipher alphabet**: alphabet used to write ciphertext (WE WILL USUALLY USE UPPER-CASE).

Spartan Scytale 400 B.C. – Transposition Cipher



Column Scytale – Transposition Cipher

- To encrypt the plaintext “attack the south gate at dawn” with 5 columns

Column Scytale – Transposition Cipher

- To encrypt the plaintext “attack the south gate at dawn” with 5 columns
- Write the text in a grid of 5 columns:

a	t	t	a	c
k	t	h	e	s
o	u	t	h	g
a	t	e	a	t
d	a	w	n	x

filling in extra space with gibberish.

Column Scytale – Transposition Cipher

- To encrypt the plaintext “attack the south gate at dawn” with 5 columns
- Write the text in a grid of 5 columns:

a	t	t	a	c
k	t	h	e	s
o	u	t	h	g
a	t	e	a	t
d	a	w	n	x

  filling in extra space with gibberish.
- Copy the ciphertext down the columns:

  AKOADTTUTATHTEWAEHANCSGTX

Columnar Transposition

- A keyword is written at the top of the columns in a table

Y	E	T	I	S	A	R	E	R	E	A	L

Columnar Transposition

- A keyword is written at the top of the columns in a table

Y	E	T	I	S	A	R	E	R	E	A	L
a	t	t	a	c	k	t	h	e	n	o	r
t	h	b	r	i	d	g	e	a	t	m	i
d	n	i	g	h	t	g	i	b	b	e	r

- Write the plaintext

  attack the north bridge at midnight

  under the keyword in rows.

Columnar Transposition

- A keyword is written at the top of the columns in a table

Y	E	T	I	S	A	R	E	R	E	A	L
a	t	t	a	c	k	t	h	e	n	o	r
t	h	b	r	i	d	g	e	a	t	m	i
d	n	i	g	h	t	g	i	b	b	e	r

- Write the plaintext

  attack the north bridge at midnight

  under the keyword in rows.
- Fill in left-over blanks with nulls or gibberish.

Columnar Transposition

- A keyword is written at the top of the columns in a table

Y	E	T	I	S	A	R	E	R	E	A	L
a	t	t	a	c	k	t	h	e	n	o	r
t	h	b	r	i	d	g	e	a	t	m	i
d	n	i	g	h	t	g	i	b	b	e	r

- Write the plaintext

  attack the north bridge at midnight

  under the keyword in rows.

- Fill in left-over blanks with nulls or gibberish.
- Re-arrange the columns to place the letters of the keyword in alphabetical order...

Columnar Transposition

A	A	E	E	E	I	L	R	R	S	T	Y
K	O	T	H	N	A	R	T	E	C	T	A
D	M	H	E	T	R	I	G	A	I	B	T
T	E	H	I	B	G	R	G	B	H	I	B

- Re-arrange the columns to place the letters of the keyword in alphabetical order...

Columnar Transposition

A	A	E	E	E	I	L	R	R	S	T	Y
K	O	T	H	N	A	R	T	E	C	T	A
D	M	H	E	T	R	I	G	A	I	B	T
T	E	H	I	B	G	R	G	B	H	I	B

- Re-arrange the columns to place the letters of the keyword in alphabetical order...
- Copy the letters down the columns to form the cipher text

Columnar Transposition

A	A	E	E	E	I	L	R	R	S	T	Y
K	O	T	H	N	A	R	T	E	C	T	A
D	M	H	E	T	R	I	G	A	I	B	T
T	E	H	I	B	G	R	G	B	H	I	B

- Re-arrange the columns to place the letters of the keyword in alphabetical order...
- Copy the letters down the columns to form the cipher text

  KDTOMETHHHEINTBARGRIRTGGEABCIHTBIATB

Columnar Transposition

A	A	E	E	E	I	L	R	R	S	T	Y
K	O	T	H	N	A	R	T	E	C	T	A
D	M	H	E	T	R	I	G	A	I	B	T
T	E	H	I	B	G	R	G	B	H	I	B

- Re-arrange the columns to place the letters of the keyword in alphabetical order...
- Copy the letters down the columns to form the cipher text

  $$KDTOMETHHHEINTBARGRIRTGGEABCIHTBIATB$$
- Reverse the steps to decrypt.

Columnar Transposition Decryption

- Decrypt this ciphertext which was encrypted with a columnar transposition with keyword CAB:

Columnar Transposition Decryption

- Decrypt this ciphertext which was encrypted with a columnar transposition with keyword CAB:

  EEXTAXRRT

Columnar Transposition Decryption

- Decrypt this ciphertext which was encrypted with a columnar transposition with keyword CAB:

  $$EEXTAXRRT$$

- Since the keyword is 3 letters and the ciphertext is 9 letters, each column has $9 \div 3 = 3 letters$

Columnar Transposition Decryption

- Decrypt this ciphertext which was encrypted with a columnar transposition with keyword CAB:

  $$EEXTAXRRT$$

- Since the keyword is 3 letters and the ciphertext is 9 letters, each column has $9 \div 3 = 3 letters$

  $$EEX, TAX, RRT$$

Columnar Transposition Decryption

- Decrypt this ciphertext which was encrypted with a columnar transposition with keyword CAB:

  $$EEXTAXRRT$$

- Since the keyword is 3 letters and the ciphertext is 9 letters, each column has $9 \div 3 = 3 letters$

  $$EEX, TAX, RRT$$

- Write columns under letters ABC (CAB in order)

A	B	C
E	T	R
E	A	R
X	X	T

Columnar Transposition Decryption

- Decrypt this ciphertext which was encrypted with a columnar transposition with keyword CAB:

  $$EEXTAXRRT$$

- Since the keyword is 3 letters and the ciphertext is 9 letters, each column has $9 \div 3 = 3 letters$

  $$EEX, TAX, RRT$$

- Write columns under letters ABC (CAB in order)

A	B	C
E	T	R
E	A	R
X	X	T

- Re-arrange

C	A	B
R	E	T
R	E	A
T	X	X

Columnar Transposition Decryption

- Decrypt this ciphertext which was encrypted with a columnar transposition with keyword CAB:

  $$EEXTAXRRT$$

- Since the keyword is 3 letters and the ciphertext is 9 letters, each column has $9 \div 3 = 3 letters$

  $$EEX, TAX, RRT$$

- Write columns under letters ABC (CAB in order)

A	B	C
E	T	R
E	A	R
X	X	T

- Re-arrange

C	A	B
R	E	T
R	E	A
T	X	X

- Read across columns to get "retreatxx"

Substitution Cipher

Make a table with the plain alphabet in the top row and the CIPHER ALPHABET in the bottom row.

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

Substitution Cipher

Make a table with the plain alphabet in the top row and the CIPHER ALPHABET in the bottom row.

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

To Encrypt: Replace each plaintext letter with the CIPHERTEXT letter beneath it in the table.

Substitution Cipher

Make a table with the plain alphabet in the top row and the CIPHER ALPHABET in the bottom row.

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

To Encrypt: Replace each plaintext letter with the CIPHERTEXT letter beneath it in the table.
To Decrypt: Replace each CIPHERTEXT with the plaintext letter above it in the table.

Substitution Cipher

Make a table with the plain alphabet in the top row and the CIPHER ALPHABET in the bottom row.

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

To Encrypt: Replace each plaintext letter with the CIPHERTEXT letter beneath it in the table.
To Decrypt: Replace each CIPHERTEXT with the plaintext letter above it in the table.
Note: The sender and receiver must both use the same table!

Caesar Cipher

Caesar Cipher

Julius Caesar used so many ciphers that Valerius Probus wrote a book about the Caesar's cryptographic methods.

Caesar Cipher

Julius Caesar used so many ciphers that Valerius Probus wrote a book about the Caesar's cryptographic methods.

- Julius Caesar used a substitution cipher in which each letter is replaced with the letter three places farther along in the alphabet. The table for this substitution would look like:

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
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

Caesar Cipher

Julius Caesar used so many ciphers that Valerius Probus wrote a book about the Caesar's cryptographic methods.

- Julius Caesar used a substitution cipher in which each letter is replaced with the letter three places farther along in the alphabet. The table for this substitution would look like:

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
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

- To make this table, place a “D” under the “a” and fill in the rest of the alphabet in order. When you get to Z, begin again with A.

Caesar Cipher

Julius Caesar used so many ciphers that Valerius Probus wrote a book about the Caesar's cryptographic methods.

- Julius Caesar used a substitution cipher in which each letter is replaced with the letter three places farther along in the alphabet. The table for this substitution would look like:

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
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

- To make this table, place a “D” under the “a” and fill in the rest of the alphabet in order. When you get to Z, begin again with A.
- There is nothing magical about “D.” You could begin with any letter.

Caesar Cipher

Julius Caesar used so many ciphers that Valerius Probus wrote a book about the Caesar's cryptographic methods.

- Julius Caesar used a substitution cipher in which each letter is replaced with the letter three places farther along in the alphabet. The table for this substitution would look like:

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
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

- To make this table, place a "D" under the "a" and fill in the rest of the alphabet in order. When you get to Z, begin again with A.
- There is nothing magical about "D." You could begin with any letter.
- Sender and receiver must begin with the same letter!

Atbash

- Ancient Hebrew cipher which appears in the Old Testament.

Atbash

- Ancient Hebrew cipher which appears in the Old Testament.
- First letter of the alphabet exchanged with last, second with second to last, and so on.

Atbash

- Ancient Hebrew cipher which appears in the Old Testament.
- First letter of the alphabet exchanged with last, second with second to last, and so on.
- Substitution table for English alphabet:

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

Substitution with keyword

A keyword can be used to help remember how to fill in a substitution table.

- To fill in the table with keyword “ICE CREAM”

Substitution with keyword

A keyword can be used to help remember how to fill in a substitution table.

- To fill in the table with keyword "ICE CREAM"
- Write keyword at beginning of CIPHER ALPHABET without repeating letters:

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
I	C	E	R	A	M																				

Substitution with keyword

A keyword can be used to help remember how to fill in a substitution table.

- To fill in the table with keyword “ICE CREAM”
- Write keyword at beginning of CIPHER ALPHABET without repeating letters:

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
I	C	E	R	A	M																				

- Write remaining letters in alphabetical order:

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

Substitution with keyword

A keyword can be used to help remember how to fill in a substitution table.

- To fill in the table with keyword "ICE CREAM"
- Write keyword at beginning of CIPHER ALPHABET without repeating letters:

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
I	C	E	R	A	M																				

- Write remaining letters in alphabetical order:

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

- If keyword does not contain letters near the end of the alphabet, then this type of substitution may not change those letters.

Monoalphabetic Substitution Ciphers

- The substitution ciphers we are considering (so far) are *monoalphabetic*.

Monoalphabetic Substitution Ciphers

- The substitution ciphers we are considering (so far) are *monoalphabetic*.
- Every letter of the plain alphabet corresponds to exactly one letter of the cipher alphabet.

Monoalphabetic Substitution Ciphers

- The substitution ciphers we are considering (so far) are *monoalphabetic*.
- Every letter of the plain alphabet corresponds to exactly one letter of the cipher alphabet.
- Every letter of the cipher alphabet corresponds to exactly one letter of the plain alphabet.

Keys

The *key* of a simple substitution is the substitution table. Certain types of substititions have shorter keys to aid in filling out the table.

Keys

The *key* of a simple substitution is the substitution table. Certain types of substititions have shorter keys to aid in filling out the table.

- **Caesar Cipher**: Key is the letter which replaces “a”

Keys

The *key* of a simple substitution is the substitution table. Certain types of substititions have shorter keys to aid in filling out the table.

- **Caesar Cipher**: Key is the letter which replaces "a"
- **Atbash**: There is not key. Table is filled in the same way every time.

Keys

The *key* of a simple substitution is the substitution table. Certain types of substititions have shorter keys to aid in filling out the table.

- **Caesar Cipher**: Key is the letter which replaces "a"
- **Atbash**: There is not key. Table is filled in the same way every time.
- **Substitution with keyword:** Key is keyword.

Ingredients of a cipher system

plaintext

Ingredients of a cipher system

plaintext + encryption key

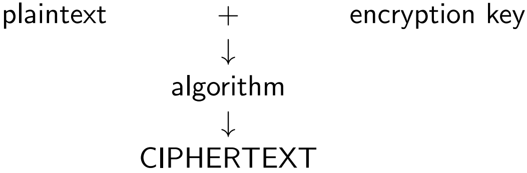
Ingredients of a cipher system

plaintext + encryption key

↓

algorithm

Ingredients of a cipher system



plaintext + encryption key

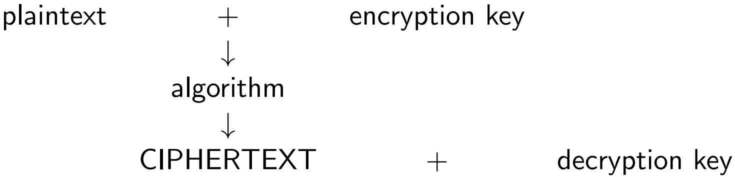
↓

algorithm

↓

CIPHERTEXT

Ingredients of a cipher system



plaintext + encryption key

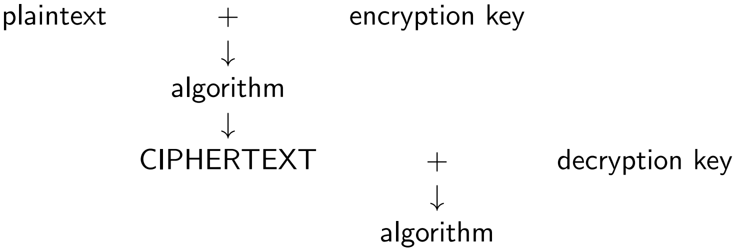
↓

algorithm

↓

CIPHERTEXT + decryption key

Ingredients of a cipher system



plaintext + encryption key

↓

algorithm

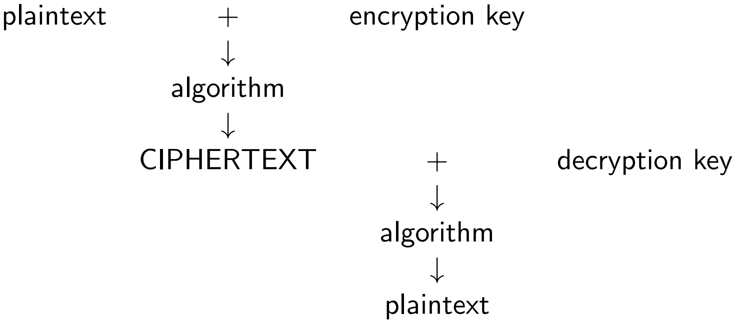
↓

CIPHERTEXT + decryption key

↓

algorithm

Ingredients of a cipher system



plaintext + encryption key

↓

algorithm

↓

CIPHERTEXT + decryption key

↓

algorithm

↓

plaintext

Source of security

Where does security come from?

Source of security

Where does security come from?
Any cipher can be broken by trying every possible key until the algorithm gives sensible plaintext.

Source of security

Where does security come from?
Any cipher can be broken by trying every possible key until the algorithm gives sensible plaintext.
For security, a cipher system needs:

Source of security

Where does security come from?
Any cipher can be broken by trying every possible key until the algorithm gives sensible plaintext.
For security, a cipher system needs:

- There should be *many* keys to choose from.

Source of security

Where does security come from?
Any cipher can be broken by trying every possible key until the algorithm gives sensible plaintext.
For security, a cipher system needs:

- There should be *many* keys to choose from.
- The key(s) should be kept absolutely secret.

Simple Substitution Ciphers were adequate for political, military, and domestic use around the world until around 1000 AD.

Some of the greatest minds in the world prior to that time believed simple substitutions to be unbreakable.

East vs West

Between 800 and 1200, the Western World (Europe) was experiencing its "Dark Ages."

Much of the Near East was experiencing a "Golden Age" marked by internal peace and prosperity.

Peace breeds cryptographers too

Peace and prosperity lead to

Peace breeds cryptographers too

Peace and prosperity lead to

- Commerce

Peace breeds cryptographers too

Peace and prosperity lead to

- Commerce
- Industry

Peace breeds cryptographers too

Peace and prosperity lead to

- Commerce
- Industry
- Academics

These require

Peace breeds cryptographers too

Peace and prosperity lead to

- Commerce
- Industry
- Academics

These require

- Administration

Peace breeds cryptographers too

Peace and prosperity lead to

- Commerce
- Industry
- Academics

These require

- Administration
- Record keeping

Peace breeds cryptographers too

Peace and prosperity lead to

- Commerce
- Industry
- Academics

These require

- Administration
- Record keeping
- Privacy

A contribution from Islam

Scholars studied the *Hadīth*, the daily sayings of Muhammad, looking closely to establish:

A contribution from Islam

Scholars studied the *Hadīth*, the daily sayings of Muhammad, looking closely to establish:

- The order of the sayings and

A contribution from Islam

Scholars studied the *Hadīth*, the daily sayings of Muhammad, looking closely to establish:

- The order of the sayings and
- Which sayings are authentic.

A contribution from Islam

Scholars studied the *Hadīth*, the daily sayings of Muhammad, looking closely to establish:

- The order of the sayings and
- Which sayings are authentic.

They counted

A contribution from Islam

Scholars studied the *Hadīth*, the daily sayings of Muhammad, looking closely to establish:

- The order of the sayings and
- Which sayings are authentic.

They counted

- words

A contribution from Islam

Scholars studied the *Hadīth*, the daily sayings of Muhammad, looking closely to establish:

- The order of the sayings and
- Which sayings are authentic.

They counted

- words
- phrases

A contribution from Islam

Scholars studied the *Hadīth*, the daily sayings of Muhammad, looking closely to establish:

- The order of the sayings and
- Which sayings are authentic.

They counted

- words
- phrases
- letters

A contribution from Islam

Scholars studied the *Hadīth*, the daily sayings of Muhammad, looking closely to establish:

- The order of the sayings and
- Which sayings are authentic.

They counted

- words
- phrases
- letters

and they noticed patterns...which lead to the invention of STATISTICS and CRYPTANALYSIS.

Patterns in a text's words, phrases, and letters can be exploited to break simple substitution ciphers.

Patterns in a text's words, phrases, and letters can be exploited to break simple substitution ciphers.

The earliest recorded description of this comes from Abū Yūsūf Ya‘qūb ibn Is-hāq ibn as-Sabbāh ibn ‘omrān ibn Ismaīl al-Kindī

Patterns in a text’s words, phrases, and letters can be exploited to break simple substitution ciphers.

The earliest recorded description of this comes from
Abū Yūsūf Ya‘qūb ibn Is-hāq ibn as-Sabbāh ibn ‘omrān ibn Ismaīl al-Kindī

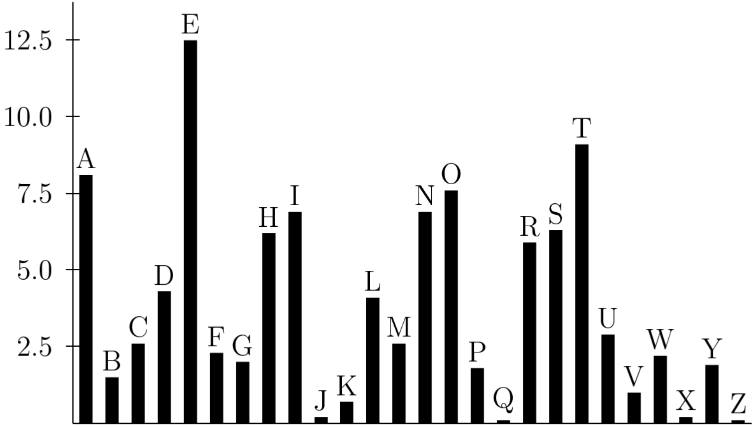
Working in the 800’s, al-Kindī wrote 300 books on medicine, astronomy, mathematics, linguistics, and music.

Letter Frequency

In most pieces of text written in English, letters do not show up with the same frequency.

Letter Frequency

In most pieces of text written in English, letters do not show up with the same frequency.



Letter Frequency

- Most common letters: E T A O N I S H R D

Letter Frequency

- Most common letters: E T A O N I S H R D
- Most common double letters: LL TT EE SS OO

Letter Frequency

- Most common letters: E T A O N I S H R D
- Most common double letters: LL TT EE SS OO
- Most common digrams: TH HE IN ER AN RE ES ND EN ON

Letter Frequency

- Most common letters: E T A O N I S H R D
- Most common double letters: LL TT EE SS OO
- Most common digrams: TH HE IN ER AN RE ES ND EN ON
- Most common trigrams: THE AND ING HER THA ERE HAT ENT ETH NTH