Complexity and Cryptography

Thomas Zeugmann

Hokkaido University
Laboratory for Algorithmics

https://www-alg.ist.hokudai.ac.jp/~thomas/COCRB/

Lecture 11: Classical Two-Way Cryptosystems

Before we start

Question

Why do we need cryptography?

Before we start

Question

Why do we need cryptography?

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.

Bruce Schneier, Applied Cryptography, Preface
John Wiley & Sons, 1996
暗号技術大全(単行本), ブルース・シュナイアー

Before we start

Question

Why do we need cryptography?

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.

Bruce Schneier, Applied Cryptography, Preface
John Wiley & Sons, 1996
暗号技術大全(単行本), ブルース・シュナイアー

We shall mainly deal with the latter.

Before you start

First, make sure that there are neither viruses nor spyware on your computer.

Before you start

First, make sure that there are neither viruses nor spyware on your computer.

There are viruses whose purpose is to intercept text between the keyboard and the computer. Then they forward the text to third-party locations.

So, even the best cryptographic tools will not help if your correspondence is intercepted pre-encryption. Spyware may be even worse.

Before you start

First, make sure that there are neither viruses nor spyware on your computer.

There are viruses whose purpose is to intercept text between the keyboard and the computer. Then they forward the text to third-party locations.

So, even the best cryptographic tools will not help if your correspondence is intercepted pre-encryption. Spyware may be even worse.

Install and use GnuPG. It is available from

`http://www.gnupg.org/`

Two famous opinions

"Ceux qui se vantent de lire les lettres chifrées sont de plus grands charlatans que ceux qui se vanteraient d'entendre une langue qu'ils n'ont point apprise."

Voltaire (Dictionnaire philosophique, 1769)

"It may be well doubted whether human ingenuity can construct an enigma of this kind [a cryptogram] which human ingenuity may not, by proper application, resolve."

E. A. Poe, (*in* The Gold Bug, 1843)

Two famous opinions

"Ceux qui se vantent de lire les lettres chifrées sont de plus grands charlatans que ceux qui se vanteraient d'entendre une langue qu'ils n'ont point apprise."

Voltaire (Dictionnaire philosophique, 1769)

"It may be well doubted whether human ingenuity can construct an enigma of this kind [a cryptogram] which human ingenuity may not, by proper application, resolve."

E. A. Poe, (*in* The Gold Bug, 1843)

Part of the course is devoted to finding out who of those famous thinkers is closer to the truth.

Cryptology I

This lectures mainly clarifies the subject of *cryptology*.
Generally speaking, cryptology is about *communication in the presence of adversaries*.
Cryptology can be diveded into two major parts, i.e., *cryptography* and *cryptanalysis*.

Cryptology I

This lectures mainly clarifies the subject of *cryptology*.
Generally speaking, cryptology is about *communication in the presence of adversaries*.
Cryptology can be diveded into two major parts, i.e., *cryptography* and *cryptanalysis*.

Cryptography is the science or art of secret writing while cryptanalysis is its natural counterpart, that is, the art of reading secret messages. A classic goal of cryptography is *privacy*: two or more parties wish to communicate in a way such that an adversary knows nothing about what was communicated.

The Basic Model I

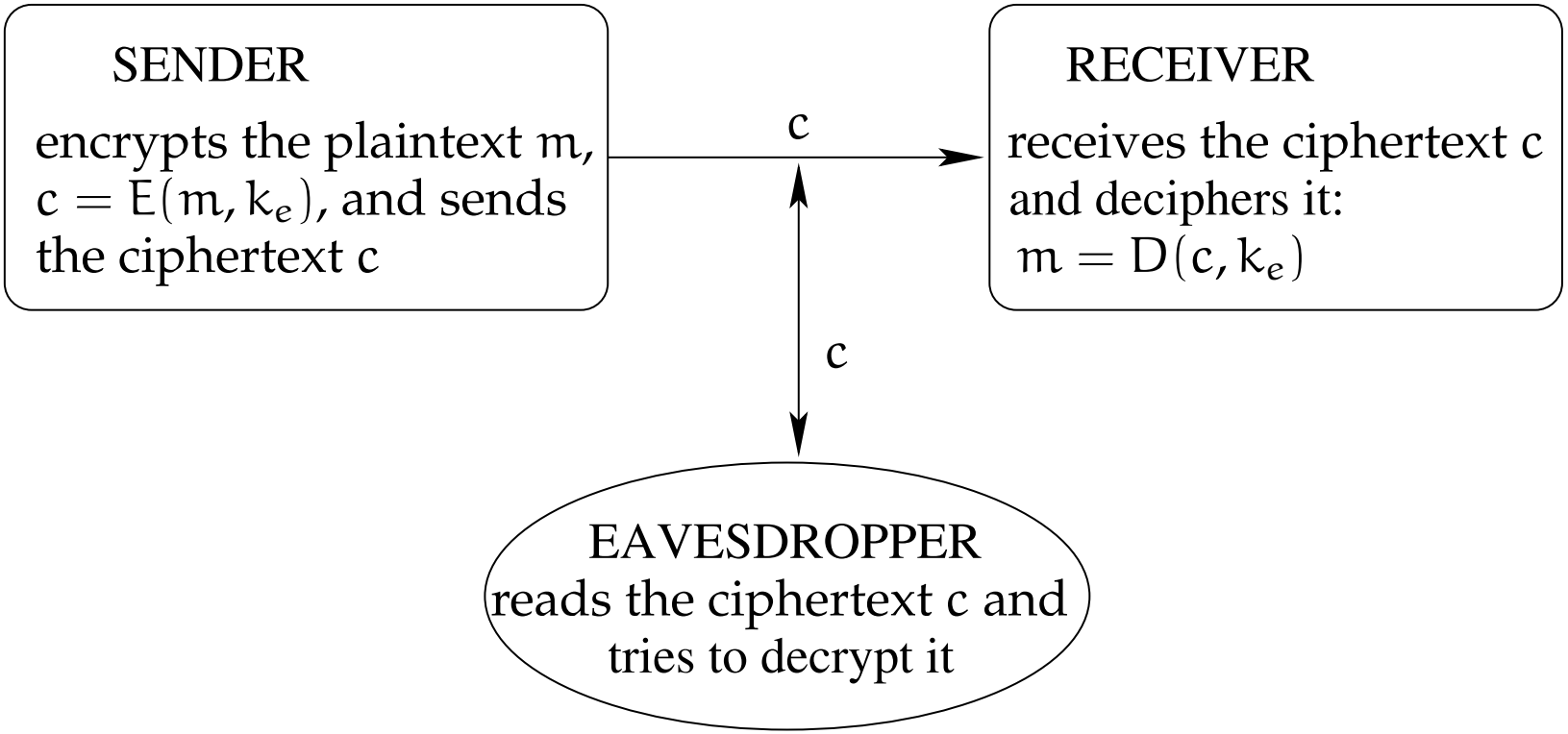


Figure 1: The Basic Model

The Basic Model II

The message we want send is called *plaintext*. However, only the intended recipients should be able to read and to understand the message sent. Thus, messages are sent in disguised form, and the disguised message is called the *ciphertext*.

The Basic Model II

The message we want send is called *plaintext*. However, only the intended recipients should be able to read and to understand the message sent. Thus, messages are sent in disguised form, and the disguised message is called the *ciphertext*.

The process of converting a plaintext to a ciphertext is called *enciphering* or *encryption*, and the reverse process is referred to as *deciphering* or *decryption*.

The Basic Model II

The message we want send is called *plaintext*. However, only the intended recipients should be able to read and to understand the message sent. Thus, messages are sent in disguised form, and the disguised message is called the *ciphertext*.

The process of converting a plaintext to a ciphertext is called *enciphering* or *encryption*, and the reverse process is referred to as *deciphering* or *decryption*.

We are confronted with contradictory requirements. Encryption and decryption should be "easy;" i.e., they should be computable using a reasonable amount of space and time. On the other hand, decryption should be "hard;" i.e., the adversary should either not be able to decipher the message eavesdropped in principal or it should be computationally infeasible for her to do so.

Caesar's System I

We exemplify this basic model using a cryptosystem invented by Julius Caesar.

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

Figure 2: The Caesar system

A plaintext is easily encrypted by replacing each letter in it by the corresponding letter displayed in the second row of the above Figure, i.e., A is replaced by Y, B is replaced by Z and so on. For example, WHY is encrypted into TEV.

The secret key is just the table above. Decryption is just the opposite.

Cryptanalysis I

This cryptosystem fulfills the first two requirements established above, i.e., encryption and deciphering are easy to compute provided the table is known.

Question

Does it also fulfill the 3rd requirement?
What can be said about the complexity of cryptanalysis in this case?

Cryptanalysis I

This cryptosystem fulfills the first two requirements established above, i.e., encryption and deciphering are easy to compute provided the table is known.

Question

Does it also fulfill the 3rd requirement?
What can be said about the complexity of cryptanalysis in this case?

Answering these questions requires some care. We have two distinguish two cases.

Cryptanalysis I

This cryptosystem fulfills the first two requirements established above, i.e., encryption and deciphering are easy to compute provided the table is known.

Question

Does it also fulfill the 3rd requirement?
What can be said about the complexity of cryptanalysis in this case?

Answering these questions requires some care. We have two distinguish two cases.
Case 1. The cryptosystem itself is unknown.
Case 2. The principal cryptosystem is known but the actual key is is unknown.

Cryptanalysis II

In the following, we always assume Case 2.
There are the following reasons to do so:

Cryptanalysis II

In the following, we always assume Case 2.
There are the following reasons to do so:

1. If a cryptosystem is hard to break in Case 2, it is even harder to break in Case 1. Thus, we are on the safer side when assuming Case 2.

Cryptanalysis II

In the following, we always assume Case 2.
There are the following reasons to do so:

1. If a cryptosystem is hard to break in Case 2, it is even harder to break in Case 1. Thus, we are on the safer side when assuming Case 2.
2. The experience gained shows that the principal structure of a cryptosystem cannot be kept secret for a long time. Thus, we are again safer when assuming Case 2.

Cryptanalysis II

In the following, we always assume Case 2.
There are the following reasons to do so:

1. If a cryptosystem is hard to break in Case 2, it is even harder to break in Case 1. Thus, we are on the safer side when assuming Case 2.
2. The experience gained shows that the principal structure of a cryptosystem cannot be kept secret for a long time. Thus, we are again safer when assuming Case 2.

So, we follow Kerckhoffs' (1883) principle: *A cryptosystem is secure, if one, knowing the cryptosystem and the algorithms used, cannot decipher the cryptotext and obtain the plaintext unless the key used is known.*

Cryptanalysis III

We generally distinguish the following sources of information available to an eavesdropper: Her task is to decipher the whole messages or at least part of them.

Cryptanalysis III

We generally distinguish the following sources of information available to an eavesdropper: Her task is to decipher the whole messages or at least part of them.

Case 2.1. Ciphertext only.

In this scenario the adversary has eavesdropped messages encrypted by using the same key.

Cryptanalysis III

We generally distinguish the following sources of information available to an eavesdropper: Her task is to decipher the whole messages or at least part of them.

Case 2.1. Ciphertext only.

In this scenario the adversary has eavesdropped messages encrypted by using the same key.

Case 2.2. Ciphertext obtained from known plaintext.

Now, the adversary has additionally access to some message in plaintext (or part of a longer message) and knows its particular encryption. This variant appears most often in practical situations.

Cryptanalysis III

We generally distinguish the following sources of information available to an eavesdropper: Her task is to decipher the whole messages or at least part of them.

Case 2.1. Ciphertext only.

In this scenario the adversary has eavesdropped messages encrypted by using the same key.

Case 2.2. Ciphertext obtained from known plaintext.

Now, the adversary has additionally access to some message in plaintext (or part of a longer message) and knows its particular encryption. This variant appears most often in practical situations.

Case 2.3. Ciphertext obtained from plaintext *chosen* by the adversary.

In this scenario, the adversary has been able to force the sender to encrypt some plaintext carefully chosen by herself.

Cryptanalysis IV

As we shall see later, the third scenario is also well conceivable, and part of the design of a cryptosystem has to be devoted to avoid such attacks to a large extent.

Now, let us attack Caesar's system.

Cryptanalysis IV

As we shall see later, the third scenario is also well conceivable, and part of the design of a cryptosystem has to be devoted to avoid such attacks to a large extent.
Now, let us attack Caesar's system.

Caesar's cryptosystem is nothing else than a cyclical shift of the alphabet $\mathcal{A}$. Thus, knowing the cipher of *one letter* is already sufficient to break it.

Cryptanalysis IV

As we shall see later, the third scenario is also well conceivable, and part of the design of a cryptosystem has to be devoted to avoid such attacks to a large extent.
Now, let us attack Caesar's system.

Caesar's cryptosystem is nothing else than a cyclical shift of the alphabet $\mathcal{A}$. Thus, knowing the cipher of *one letter* is already sufficient to break it.

So, in Case 2.3 the adversary has no difficulties at all. The same applies *mutatis mutandis* to Case 2.2.

Cryptanalysis IV

As we shall see later, the third scenario is also well conceivable, and part of the design of a cryptosystem has to be devoted to avoid such attacks to a large extent.
Now, let us attack Caesar's system.

Caesar's cryptosystem is nothing else than a cyclical shift of the alphabet $\mathcal{A}$. Thus, knowing the cipher of *one letter* is already sufficient to break it.

So, in Case 2.3 the adversary has no difficulties at all. The same applies *mutatis mutandis* to Case 2.2.

There are only 27 cyclical shifts. Thus, even in Case 2.1 the adversary has no principal difficulty to decipher the message received. Trying all possibilities is feasible and leads to successful encryption.

Cryptanalysis V

Observation: *Cryptosystems must be designed in a way such that the number of possible keys is huge.*

Cryptanalysis V

Observation: *Cryptosystems must be designed in a way such that the number of possible keys is huge.*

Let us again take our alphabet $\mathcal{A}$ and as the set of all possible keys we consider all permutations of $\mathcal{A}$. This would be the most general version of the Cesar system.
Thus, we have $27!$ many keys, and since $27! \leqslant 8 \cdot 10^{27}$ just trying them all is not feasible. Even if we could test 10^9 many permutations per second, this exaustive testing would take roughly 10^{11} years.

Cryptanalysis V

Observation: *Cryptosystems must be designed in a way such that the number of possible keys is huge.*

Let us again take our alphabet $\mathcal{A}$ and as the set of all possible keys we consider all permutations of $\mathcal{A}$. This would be the most general version of the Cesar system.
Thus, we have $27!$ many keys, and since $27! \leqslant 8 \cdot 10^{27}$ just trying them all is not feasible. Even if we could test 10^9 many permutations per second, this exaustive testing would take roughly 10^{11} years.

So, at first glance, everything looks fine. Unfortunately, there is a "but," and in this case it sounds "but there is frequency analysis."

Cryptanalysis VI

The background of frequency analysis is the observation that letters appear with different frequencies in natural language. For example, in German we have the following picture:

E	18.46 %	R	7.14 %	T	5.22 %
N	11.42 %	S	7.04 %	U	5.01 %
I	8.02 %	A	5.38 %	D	4.94 %

Cryptanalysis VI

The background of frequency analysis is the observation that letters appear with different frequencies in natural language. For example, in German we have the following picture:

E	18.46 %	R	7.14 %	T	5.22 %
N	11.42 %	S	7.04 %	U	5.01 %
I	8.02 %	A	5.38 %	D	4.94 %

Note that there is no absolute table for the relative frequencies of letters, since they vary in dependence on the subjects. For instance, if we compute frequencies in stock market reports and book of tales, then you get different values. Nevertheless, in German texts the letters E and N always have the highest frequency.

Cryptanalysis VII

Now, the idea of frequency analysis is to compute the frequencies in the ciphertext and to try a mapping with respect to the table displayed above. It works very often quite well.

Cryptanalysis VII

Now, the idea of frequency analysis is to compute the frequencies in the ciphertext and to try a mapping with respect to the table displayed above. It works very often quite well.

So far, we have considered cryptosystems that enciphered all plaintext message units using one and the same rule. Such cryptosystems are referred to as *monoalphabetic* systems. In contrast, in the following we study cryptosystems working as follows: The first plaintext message unit is enciphered using Rule 1, the second plaintext message unit is enciphered using Rule 2, . . . , the kth plaintext message unit is enciphered applying Rule k. In case the plaintext contains more than k plaintext message units, one applies the rules modulo k.
Such systems are called *polyalphabetic*.

The Vigenère System I

Keyword: MAGIC Message: CRYPTOLOGY

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Ciphertext:

The Vigenère System I

Keyword: MAGIC Message: CRYPTOLOGY

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Ciphertext: O

The Vigenère System I

Keyword: MAGIC Message: CRYPTOLOGY

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Ciphertext: OR

The Vigenère System I

Keyword: MAGIC Message: CRYPTOLOGY

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Ciphertext: ORE

The Vigenère System I

Keyword: MAGIC Message: CRYPTOLOGY

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Ciphertext: OREX

The Vigenère System I

Keyword: MAGIC Message: CRYPTOLOGY

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Ciphertext: OREXV

The Vigenère System I

Keyword: MAGIC Message: CRYPTOLOGY

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Ciphertext: OREXVA

The Vigenère System I

Keyword: MAGIC Message: CRYPTOLOGY

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Ciphertext: OREXVAL

The Vigenère System I

Keyword: MAGIC Message: CRYPTOLOGY

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Ciphertext: OREXVALU

The Vigenère System I

Keyword: MAGIC Message: CRYPTOLOGY

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Ciphertext: OREXVALUO

The Vigenère System I

Keyword: MAGIC Message: CRYPTOLOGY

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Ciphertext: OREXVALUOA

The Vigenère System II

Vigenère published his system in 1585 and it took roughly 300 years before it was broken. It is the periodicity of the repeating key which leads to the weaknesses in this method and its vulnerabilities to cryptanalysis. Wilhelm Kasiski published in 1863 his book *Die Geheimschriften und die Dechiffrir-Kunst* containing his famous algorithm.

Blaise de Vigenère
(1523–1596)

We therefore continue here with Kasiski's algorithm.

Kasiski's Algorithm I

Step 1. Search all words $v_0, \ldots, v_\ell$ in the ciphertext that appear at least twice in the ciphertext, i.e., search all v_i such that the ciphertext can be presented as $w_i v_i q_i v_i r_i$, where w_i, q_i, r_i are also words over the cipher alphabet.

Kasiski's Algorithm I

Step 1. Search all words $v_0, \ldots, v_\ell$ in the ciphertext that appear at least twice in the ciphertext, i.e., search all v_i such that the ciphertext can be presented as $w_i v_i q_i v_i r_i$, where w_i, q_i, r_i are also words over the cipher alphabet.

Step 2. For each v_i found, $i = 0, \ldots \ell$, compute all divisors of $|v_i q_i|$.

Kasiski's Algorithm I

Step 1. Search all words $v_0, \ldots, v_\ell$ in the ciphertext that appear at least twice in the ciphertext, i.e., search all v_i such that the ciphertext can be presented as $w_i v_i q_i v_i r_i$, where w_i, q_i, r_i are also words over the cipher alphabet.

Step 2. For each v_i found, $i = 0, \ldots \ell$, compute all divisors of $|v_i q_i|$.

Step 3. Order the divisors found in Step 2 by their frequency. Starting with the most frequent one try for each divisor a monoalphabetic attack until a "meaningful" plaintext has been discovered.

Kasiski's Algorithm II

Lemma 1 (Kasiski)

Let d be the length of the key word used. Then, for every key word of length d, the corresponding Vigenère Substitution can be decomposed into d monoalphabetic substitutions.

Proof. Let $w = s_0 \dots s_{d-1}$ be any key word of length d, and let $k_0 k_1 \dots k_m$ be the plaintext to be enciphered. We write the plaintext in blocks of length d below the key word:

$$
\begin{array}{cccc}
s_0 & s_1 & \dots & s_{d-1} \\
k_0 & k_1 & \dots & k_{d-1} \\
k_d & k_{d+1} & \dots & k_{2d-1} \\
k_{2d} & k_{2d+1} & \dots & k_{3d-1} \\
\vdots & & & \\
k_{\ell d} & k_{\ell d+1} & \dots & k_m\,.
\end{array}
$$

Kasiski's Algorithm III

Hence, all plaintext message units in column $i \in \{0, \ldots, d-1\}$ are enciphered by the same monoalphabetic substitution defined by letter s_i of the key word. More precisely, the first letter of the alphabet $\mathcal{A}$ is mapped to s_i; thus canonically defining a shift operation for the remaining letters.

Kasiski's Algorithm III

Hence, all plaintext message units in column $i \in \{0, \ldots, d-1\}$ are enciphered by the same monoalphabetic substitution defined by letter s_i of the key word. More precisely, the first letter of the alphabet $\mathcal{A}$ is mapped to s_i; thus canonically defining a shift operation for the remaining letters. ∎

So, we should give it a try. The example is from Salomaa (1990). The following ciphertext has been eavesdropped:

Kasiski's Algorithm IV

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

What does it mean?

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

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

Step 1 gives $v_0 = \text{HALVXHFMVTLHIGH}$ having $|v_0 q_0| = 375$

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

Step 1 gives ν_0 = HALVXHFMVTLHIGH having $|\nu_0 q_0| = 375$ and

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

Step 1 gives v_0 = HALVXHFMVTLHIGH having $|v_0 q_0| = 375$ and v_1 = VXHFMVTLHIGH having $|v_1 q_{1,0}| = 129$ (first and second) and $|v_1 q_{1,1}| = 246$ (second and third).

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

In Step 1 we find $|v_0 q_0| = 375$, $|v_1 q_{1,0}| = 129$, $|v_1 q_{1,1}| = 246$,

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

In Step 1 we find $|v_0 q_0| = 375$, $|v_1 q_{1,0}| = 129$, $|v_1 q_{1,1}| = 246$, and VXH (in the 6th row, with distance 12)

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

In Step 1 we find $|v_0 q_0| = 375$, $|v_1 q_{1,0}| = 129$, $|v_1 q_{1,1}| = 246$, and VXH (in the 6th row, with distance 12) and AVX with distances 141, 39, VX gives also 180,

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

In Step 1 we find $|v_0 q_0| = 375$, $|v_1 q_{1,0}| = 129$, $|v_1 q_{1,1}| = 246$, and VXH (in the 6th row, with distance 12) and AVX with distances 141, 39, VX gives also 180, and HAL with distances 246, 60, 69.

Computing Divisors

for 375: 1, 3, 5, 25, 125, 15, 75, 375,

Computing Divisors

for 375: 1, 3, 5, 25, 125, 15, 75, 375,
for 129: 1, 3, 43, 129,

Computing Divisors

for 375: 1, 3, 5, 25, 125, 15, 75, 375,
for 129: 1, 3, 43, 129,
for 246: 1, 2, 3, 41, 6, 82, 123, 246,

Computing Divisors

for 375: 1, 3, 5, 25, 125, 15, 75, 375,
for 129: 1, 3, 43, 129,
for 246: 1, 2, 3, 41, 6, 82, 123, 246,
for 180: 1, 2, 3, 4, 6, 5, 10, 15, 20, 45, 12, 36, 180,

Computing Divisors

for 375: 1, 3, 5, 25, 125, 15, 75, 375,
for 129: 1, 3, 43, 129,
for 246: 1, 2, 3, 41, 6, 82, 123, 246,
for 180: 1, 2, 3, 4, 6, 5, 10, 15, 20, 45, 12, 36, 180,
for 141: 1, 3, 47, 141,

Computing Divisors

for 375: 1, 3, 5, 25, 125, 15, 75, 375,
for 129: 1, 3, 43, 129,
for 246: 1, 2, 3, 41, 6, 82, 123, 246,
for 180: 1, 2, 3, 4, 6, 5, 10, 15, 20, 45, 12, 36, 180,
for 141: 1, 3, 47, 141,
for 60: nothing new, because 60 divides 180,

Computing Divisors

for 375: 1, 3, 5, 25, 125, 15, 75, 375,
for 129: 1, 3, 43, 129,
for 246: 1, 2, 3, 41, 6, 82, 123, 246,
for 180: 1, 2, 3, 4, 6, 5, 10, 15, 20, 45, 12, 36, 180,
for 141: 1, 3, 47, 141,
for 60: nothing new, because 60 divides 180,
for 39: 1, 3, 13, 39,

Computing Divisors

for 375: 1, 3, 5, 25, 125, 15, 75, 375,
for 129: 1, 3, 43, 129,
for 246: 1, 2, 3, 41, 6, 82, 123, 246,
for 180: 1, 2, 3, 4, 6, 5, 10, 15, 20, 45, 12, 36, 180,
for 141: 1, 3, 47, 141,
for 60: nothing new, because 60 divides 180,
for 39: 1, 3, 13, 39,
for 69: 1, 3, 23, 69, and

Computing Divisors

for 375: 1, 3, 5, 25, 125, 15, 75, 375,
for 129: 1, 3, 43, 129,
for 246: 1, 2, 3, 41, 6, 82, 123, 246,
for 180: 1, 2, 3, 4, 6, 5, 10, 15, 20, 45, 12, 36, 180,
for 141: 1, 3, 47, 141,
for 60: nothing new, because 60 divides 180,
for 39: 1, 3, 13, 39,
for 69: 1, 3, 23, 69, and
for 12: nothing new.

Kasiski's Algorithm V

Thus, 3 is the most frequent divisor found, since it divides all distances.
Moreover, since several words have been pretty long, it is highly improbable that this is just by chance.

Kasiski's Algorithm V

Thus, 3 is the most frequent divisor found, since it divides all distances.
Moreover, since several words have been pretty long, it is highly improbable that this is just by chance.

Consequently, we conjecture the key word length to be 3. In order to perform the monoalphabetical attacks, we rewrite the ciphertext in three columns as described above and obtain:

s_0 s_1 s_2	s_0 s_1 s_2	s_0 s_1 s_2	s_0 s_1 s_2	s_0 s_1 s_2	s_0 s_1 s_2	s_0 s_1 s_2
A V X	L Q H	Y M T	A V X	A V M	W Z X	L F R
Z H H	T S L	U R A	T C L	V C Y	V T L	Z A T
C S B	T C K	B A B	A Q H	L K L	A C G	S Z G
Z H A	L V N	K V X	T A H	A C G	L G H	L J X
L V X	T W W	H H B	U A B	L G B	U H H	Y P X
H F M	H B W	U G T	Z H T	M H A	W H A	Z H B
V T L	M S X	B B T	R S B	L G M	L B M	U U R
H I G	S G A	A V X	U P N	V J X	O S K	D W M
H K A	V H M	H F M	P Z W	P G H	V C F	O H A
L B R	L F R	V T L	P B Z	U Z R	J O G	L V X
V I M	V I T	H I G	H G T	H A B	U C M	H F M
O F H	Y S M	H P N	B B T	Z S K	I S A	V T L
D K T	O I L	P Z W	P G M	H P E	L O M	H I G
A S K	H P E	P B Z	V V T	L H B	L R I	H
V B M	L H H	P G G	C S M	U M F	Y C I	
O S L	L L I	V H W	V C L	L H T	L F E	
A C G	L F B	P G V	T O E	S P H	F I G	
L G M	L B V	B G L	S O L	E K B	S S L	
O S T	L P H	L R A	A C O	A V T	Z W M	
P F U	A V W	L F X	L K B	J C N	P G O	

Counting Letters

For each column s_0, s_1, s_2 counting yields:

Letter	s_0	s_1	s_2	Letter	s_0	s_1	s_2
A	12	5	9	N	0	0	4
B	4	9	12	O	6	4	2
C	2	11	0	P	10	7	0
D	2	0	0	Q	0	2	0
E	1	0	4	R	1	3	5
F	1	10	2	S	5	13	0
G	0	13	10	T	6	4	13
H	15	14	11	U	9	1	1
I	1	7	3	V	14	11	2
J	2	2	0	W	2	3	6
K	1	5	4	X	0	1	12
L	27	1	13	Y	4	0	1
M	2	2	17	Z	7	5	2

Statistical Information for English

E	12.31 %	O	7.94 %	S	6.59 %
T	9.59 %	N	7.19 %	R	6.03 %
A	8.05 %	I	7.18 %	H	5.14 %

But the ciphertext received has been pretty short.

Statistical Information for English

E	12.31 %	O	7.94 %	S	6.59 %
T	9.59 %	N	7.19 %	R	6.03 %
A	8.05 %	I	7.18 %	H	5.14 %

But the ciphertext received has been pretty short.

Refinement: triple RST is the only of consecutive letters that all have high frequency.

Statistical Information for English

E	12.31 %	O	7.94 %	S	6.59 %
T	9.59 %	N	7.19 %	R	6.03 %
A	8.05 %	I	7.18 %	H	5.14 %

But the ciphertext received has been pretty short.

Refinement: triple RST is the only of consecutive letters that all have high frequency.

Idea: search for triples of consecutive letters having simultaneously high frequency.

Statistical Information for English

E	12.31 %	O	7.94 %	S	6.59 %
T	9.59 %	N	7.19 %	R	6.03 %
A	8.05 %	I	7.18 %	H	5.14 %

But the ciphertext received has been pretty short.

Refinement: triple RST is the only of consecutive letters that all have high frequency.

Idea: search for triples of consecutive letters having simultaneously high frequency.

There are two such triples: TUV and YZA

Looking at TUV and YZA

Letter	s_0	s_1	s_2	Letter	s_0	s_1	s_2
A	12	5	9	N	0	0	4
B	4	9	12	O	6	4	2
C	2	11	0	P	10	7	0
D	2	0	0	Q	0	2	0
E	1	0	4	R	1	3	5
F	1	10	2	S	5	13	0
G	0	13	10	T	6	4	13
H	15	14	11	U	9	1	1
I	1	7	3	V	14	11	2
J	2	2	0	W	2	3	6
K	1	5	4	X	0	1	12
L	27	1	13	Y	4	0	1
M	2	2	17	Z	7	5	2

Relooking at TUV and YZA

Assuming $\mathbf{R} \rightarrow \mathbf{T}$, $\mathbf{S} \rightarrow \mathbf{U}$, and $\mathbf{T} \rightarrow \mathbf{V}$ results in conjecturing a monoalphabetic right shift by two positions, i.e.,

Relooking at TUV and YZA

Assuming $\mathbf{R} \rightarrow \mathbf{T}$, $\mathbf{S} \rightarrow \mathbf{U}$, and $\mathbf{T} \rightarrow \mathbf{V}$ results in conjecturing a monoalphabetic right shift by two positions, i.e.,

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
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

Relooking at TUV and YZA

Assuming $\mathbf{R} \longrightarrow \mathbf{T}$, $\mathbf{S} \longrightarrow \mathbf{U}$, and $\mathbf{T} \longrightarrow \mathbf{V}$ results in conjecturing a monoalphabetic right shift by two positions, i.e.,

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
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

Thus, Y, Z, and A would be the image of W, X, and Y, respectively. Consequently, the letters W, X, and Y must appear 4, 7, and 12 times, respectively, in the plaintext. This seems highly unlikely.

Relooking at TUV and YZA

Assuming **R** $\rightarrow$ **T**, **S** $\rightarrow$ **U**, and **T** $\rightarrow$ **V** results in conjecturing a monoalphabetic right shift by two positions, i.e.,

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
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

Thus, Y, Z, and A would be the image of W, X, and Y, respectively. Consequently, the letters W, X, and Y must appear 4, 7, and 12 times, respectively, in the plaintext. This seems highly unlikely.

Therefore, we favor **R** $\rightarrow$ **Y**, **S** $\rightarrow$ **Z**, and **T** $\rightarrow$ **A** resulting in:

Relooking at TUV and YZA

Assuming $\mathbf{R} \rightarrow \mathbf{T}$, $\mathbf{S} \rightarrow \mathbf{U}$, and $\mathbf{T} \rightarrow \mathbf{V}$ results in conjecturing a monoalphabetic right shift by two positions, i.e.,

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
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

Thus, Y, Z, and A would be the image of W, X, and Y, respectively. Consequently, the letters W, X, and Y must appear 4, 7, and 12 times, respectively, in the plaintext. This seems highly unlikely.

Therefore, we favor $\mathbf{R} \rightarrow \mathbf{Y}$, $\mathbf{S} \rightarrow \mathbf{Z}$, and $\mathbf{T} \rightarrow \mathbf{A}$ resulting in:

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
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

Looking at the 2nd Column

We find ABC and FGH (possibly ZAB and GHI, too; but they are less probable). Using similar arguments as above, ABC is less probable than FGH. Thus, we continue working with

Looking at the 2nd Column

We find ABC and FGH (possibly ZAB and GHI, too; but they are less probable). Using similar arguments as above, ABC is less probable than FGH. Thus, we continue working with

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
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

Looking at the 3rd Column

Here, KLM and FGH are possible candidates. First, we favor KLM; thus obtaining:

Looking at the 3rd Column

Here, KLM and FGH are possible candidates. First, we favor KLM; thus obtaining:

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
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

Putting it all Together

Our three conjectures

$$\begin{aligned} t_0(x) &= x + 7 \mod 26, \\ t_1(x) &= x + 14 \mod 26, \\ t_2(x) &= x + 19 \mod 26, \end{aligned}$$

i.e.,

Putting it all Together

Our three conjectures

$$\begin{aligned} t_0(x) &= x + 7 \mod 26, \\ t_1(x) &= x + 14 \mod 26, \\ t_2(x) &= x + 19 \mod 26, \end{aligned}$$

i.e.,

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
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
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
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

Putting it all Together

Our three conjectures

$$\begin{aligned} t_0(x) &= x + 7 \mod 26, \\ t_1(x) &= x + 14 \mod 26, \\ t_2(x) &= x + 19 \mod 26, \end{aligned}$$

i.e.,

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
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
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
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

provide the key word HOT.

Deciphering

Keyword: HOT Ciphertext: AVXZHHCSBZHALVXHFMVTLHIGH

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Plaintext: T

Deciphering

Keyword: HOT Ciphertext: AVXZHHCSBZHALVXHFMVTLHIGH

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Plaintext: TH

Deciphering

Keyword: HOT Ciphertext: AVXZHHCSBZHALVXHFMVTLHIGH

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Plaintext: THE

Deciphering

Keyword: HOT Ciphertext: AVXZHHCSBZHALVXHFMVTLHIGH

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Plaintext: THES

Deciphering

Keyword: HOT Ciphertext: AVXZHHCSBZHALVXHFMVTLHIGH

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Plaintext: THEST

Deciphering

Keyword: HOT Ciphertext: AVXZHHCSBZHALVXHFMVTLHIGH

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Plaintext: THESTO

Deciphering

Keyword: HOT Ciphertext: AVXZHHCSBZHALVXHFMVTLHIGH

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Plaintext: THESTOV

Deciphering

Keyword: HOT Ciphertext: AVXZHHCSBZHALVXHFMVTLHIGH

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Plaintext: THESTOVE

Deciphering

Keyword: HOT Ciphertext: AVXZHHCSBZHALVXHFMVTLHIGH

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Plaintext: THESTOVEI

Deciphering

Keyword: HOT Ciphertext: AVXZHHCSBZHALVXHFMVTLHIGH

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Plaintext: THESTOVEIS

Deciphering

Keyword: HOT Ciphertext: AVXZHHCSBZHALVXHFMVTLHIGH

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Plaintext: THESTOVEIST

Deciphering

Keyword: HOT Ciphertext: AVXZHHCSBZHALVXHFMVTLHIGH

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Plaintext: THESTOVEISTHEHEARTOFSAUNA...

Inserting Blanks

THE STOVE IS THE HEART OF SAUNA

WHEN YOU THROW . . .

Inserting Blanks

THE STOVE IS THE HEART OF SAUNA

WHEN YOU THROW . . .

Wow, that's a message about sauna.

Complete Solution

"The stove is the heart of sauna. When you throw water on the stones, the air becomes more humid and feels hotter. You are thus able to experience both dry and humid heat in sauna. The art of sauna building is not discussed here. The most common mistake in building a sauna is to have too small a stove with too few stones. If the stove is only a miserable tiny metal box with a couple of stones on the top, then the room cannot be heated properly unless it is very small. Never be stingy with the heart of sauna."

Final Remarks

VXH appeared thrice in ciphertext.

Final Remarks

VXH appeared thrice in ciphertext.

VXH constitutes the cipher of HEA.

Final Remarks

VXH appeared thrice in ciphertext.

VXH constitutes the cipher of HEA.

But, the different appearances of VXH in the ciphertext stem from

Final Remarks

VXH appeared thrice in ciphertext.

VXH constitutes the cipher of HEA.

But, the different appearances of VXH in the ciphertext stem from

HEART, HEATING and THEART.

Final Remarks

VXH appeared thrice in ciphertext.

VXH constitutes the cipher of HEA.

But, the different appearances of VXH in the ciphertext stem from

HEART, HEATING and THEART.

So, there was a bit luck for deciphering the text.

Final Remarks

VXH appeared thrice in ciphertext.

VXH constitutes the cipher of HEA.

But, the different appearances of VXH in the ciphertext stem from

HEART, HEATING and THEART.

So, there was a bit luck for deciphering the text.

On the other hand, the most frequent letters in each class have been E, T, A, O, N, I, S, H, R.
Thus, the keyword was much too short for the plaintext.

Final Remarks

Kahn credits Giovan Batista Belaso (1553) for having "proposed the use of a literal, easily remembered, and easily changed key . . . for a polyalphabetic cipher," for what we know today as the Vigenère cipher.

Final Remarks

Kahn credits Giovan Batista Belaso (1553) for having "proposed the use of a literal, easily remembered, and easily changed key . . . for a polyalphabetic cipher," for what we know today as the Vigenère cipher.

According to Kahn, Vigenère himself developed a far more sophisticated system, an "autokey" that uses the plaintext as its own key. For example, if we want to encrypt

Final Remarks

Kahn credits Giovan Batista Belaso (1553) for having "proposed the use of a literal, easily remembered, and easily changed key . . . for a polyalphabetic cipher," for what we know today as the Vigenère cipher.

According to Kahn, Vigenère himself developed a far more sophisticated system, an "autokey" that uses the plaintext as its own key. For example, if we want to encrypt

```
THIS IS A SECRET MESSAGE
```

Final Remarks

Kahn credits Giovan Batista Belaso (1553) for having "proposed the use of a literal, easily remembered, and easily changed key . . . for a polyalphabetic cipher," for what we know today as the Vigenère cipher.

According to Kahn, Vigenère himself developed a far more sophisticated system, an "autokey" that uses the plaintext as its own key. For example, if we want to encrypt

`THIS IS A SECRET MESSAGE`

we choose a secret seed key character, say "D," and we write:

Final Remarks

Kahn credits Giovan Batista Belaso (1553) for having "proposed the use of a literal, easily remembered, and easily changed key . . . for a polyalphabetic cipher," for what we know today as the Vigenère cipher.

According to Kahn, Vigenère himself developed a far more sophisticated system, an "autokey" that uses the plaintext as its own key. For example, if we want to encrypt

```
THIS IS A SECRET MESSAGE
```

we choose a secret seed key character, say "D," and we write:

```
autokey:    DTHISISASECRETMESSAG
message:    THISISASECRETMESSAGE
```

Final Remarks

Kahn credits Giovan Batista Belaso (1553) for having "proposed the use of a literal, easily remembered, and easily changed key . . . for a polyalphabetic cipher," for what we know today as the Vigenère cipher.

According to Kahn, Vigenère himself developed a far more sophisticated system, an "autokey" that uses the plaintext as its own key. For example, if we want to encrypt

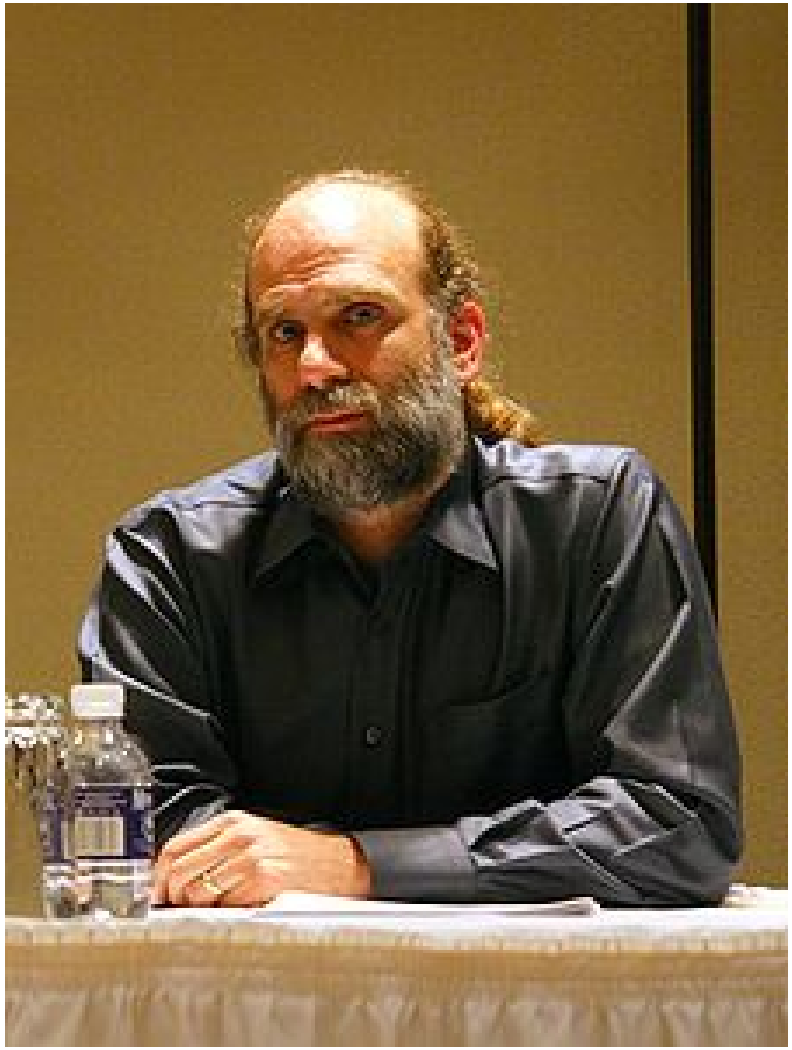
```
THIS IS A SECRET MESSAGE
```

we choose a secret seed key character, say "D," and we write:

```
autokey:    DTHISISASECRETMESSAG
message:    THISISASECRETMESSAGE
```

Additionally, Vigenère proposed scrambling the row and column indexing alphabets at the top and side. This scrambling plus the seed character would form what we would consider the "secret key" nowadays.

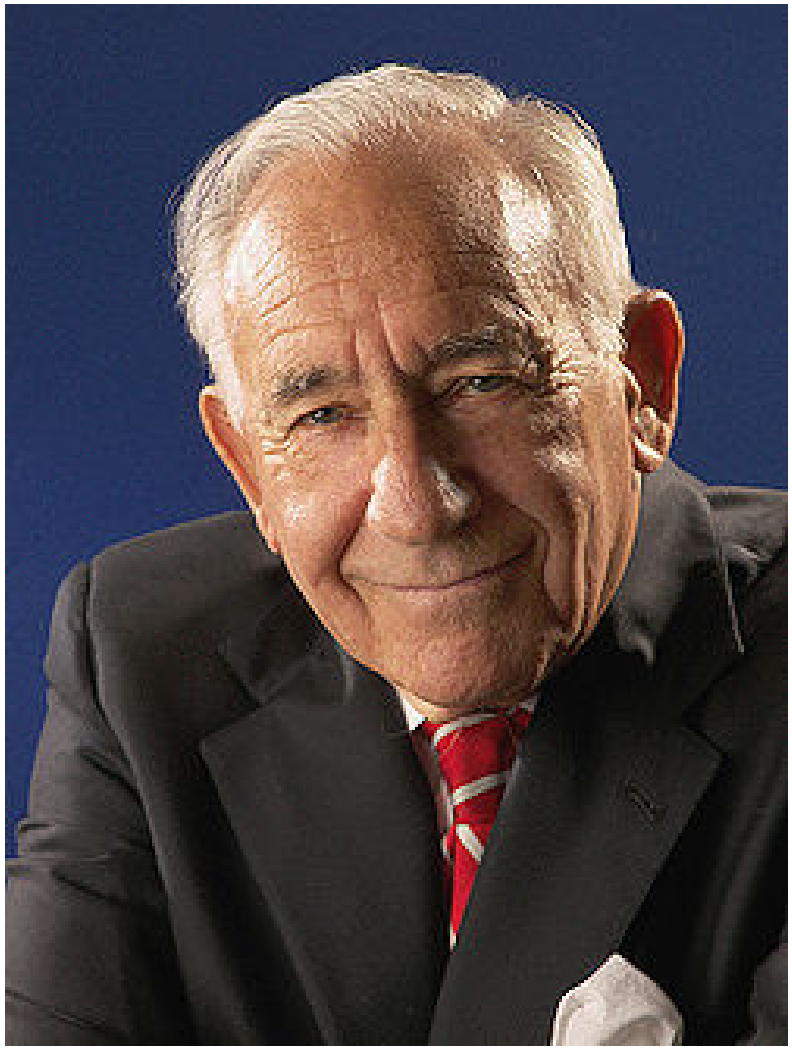
Thank you!



Bruce Schneier

Julius Caesar

Auguste Kerckhoffs



David Kahn