



Cryptography Enriched by the Art of Music

Tonislav Svetoslavov Troev
Konstantin Preslavski University of
Shumen



What is "cryptography"?

- Cryptography studies the principles, tools and methodologies for securing the open communication channels whenever there is presence of third parties that are not eligible of accessing the transmitted information.
- Prior to the 20th century cryptography describes the process of converting some intelligible information into unintelligible nonsense. The sender encrypts the data and shares the decoding technology only with the intended recipient. Thus, if any adversary gets access to the sent text, it will not have any semantic value.



Related studies

- "Steganography" is a study of hiding the existence of secret information. One of the earliest historical examples is described by Herodotus - a secret message is tattooed on the head of a slave and later it is concealed by his regrown hair. Nowadays, steganography is used to conceal data (in any format - text, image, sound, etc.) within digital files.
- "Cryptanalysis" is the study that tries to gain access to the content of the encrypted information without knowing the cryptographic mechanism being used and respectively - neither of the encryption or decryption keys.

History of cryptography

- One of the oldest types of ciphers being used in Ancient Greece, Egypt and Rome are the so called "transposition" and "substitution" ciphers.
- The transposition ciphers only change the position of the message's units (letters, pair of letters, triplets or any other group of letters).
- The substitution ciphers only change the message's units without rearranging their position.

One of the oldest cryptography tools used by Ancient Greeks and Spartans. It is called "skytale". The secret text is written on some material wrapped around a stick. This is a transpositional cipher and its key is actually the stick itself - its shape and thickness.



History of cryptography

- In the last century new branches of cryptography were discovered, developed and integrated within many aspects of our life. The new methods of data protection have become more complex than ever before and there are two main reasons for this:
 - World War I and World War II. During devastating wars it would be a fatal mistake if your enemies know what is your plan and on the battlefield there is no place for mistakes. Rotor cipher machines were developed and used before WWI. On the other hand, "Enigma" is one of the most known machines used by the nazis. It took years for cryptanalysts to understand how it works and how to potentially decode the secret information sent from German officers. The breaking of this cipher altered the course of WWII.
 - Rapid digitalization. Computers have helped us to automate various processes that led to the rise of cryptanalysis but they also made the existence of a lot more complex ciphers possible because of their computation power. "Colossus" is the first computer that assisted in the decryption of ciphers generated by the German Army's machines.

Examples of Transposition ciphers

It is a common practice to add "null" values that can be randomly selected letters (or group of letters according to the used cryptography mechanism) in order to fill in the left spaces. After the message is decoded, they will have no semantic value.

The encoded text can also be grouped in any manner - in groups of five letters, in groups of three letters, etc. For simplicity, in the following examples there is no grouping.

Rail fence cipher

```
Plain text: Good morning
Key: 4 (The number of used rows)

G.....r....
.o...o.n...
..o.m...i.g
...d.....n.
Encoded text: Groomigdn
```

Skytale cipher

```
Plain text: Welcome home
Key: 2 (The number of used rows)

W.e.l.c.o.m
.e.h.o.m.e.
Encoded text: Weehlocmoem
```

Columnar transposition

```
Plain text: Outside the view is beautiful.
Keys:
- The number of columns: 4
- Keyword: CORN
```

The alphabetical ordering of the chosen keyword's letters defines the order of the columns.

```
1 3 4 2
O u t s
i d e t
h e v i
e w i s
b e a u
t i f u
l x y z
Encoded text: Oihebtlstisuuzudeweixteviafy
```

Examples of Substitution ciphers

Caesar cipher

```
Plain text: It has been raining for the last two weeks.  
Key: -3  
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  
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  
Encoded text: Fq exp ybbk oxfkfkd clo qeb ixoq qtl tbbhp.
```

Atbash cipher

```
Plain text: I will visit Paris in October.  
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  
Encoded text: R droo erhrg Kzirh rm Lxglyvi.
```

Modern cryptography

In modern cryptography there are three major types of algorithms being used:

- **Symmetric-key algorithms.** The key used for encoding and decoding is the same and this is one of the biggest drawbacks of this type of algorithms because every member of the secret conversation should have access to the private key.
- **Assymmetric-key algorithms.** The algorithms in this group (also known as "public-key cryptography") use two keys – a public-key (assymmetric-key) for encryption and a private-key for decryption. The public-key can be freely shared and that will not affect the security state of the communication in any way but the private key should be stored in secret. The assymmetric-key algorithms do have a vast application – they are in the core of network security schemes like "TLS/SSL" - the security layer of "Hypertext transfer protocol secure" (HTTPS) that is a standard for secure communication over the Internet.
- **Hash functions.** Cryptographic hash functions are one-way functions meaning that if we have the hash of some message, we cannot know its original value (the computations cannot be reversed). If authentication is required, hash functions should be used. For example, every well written software should not store the passwords of the registered users in plain text form as they will not be secure. Instead, the passwords are hashed and then stored in a database (it is possible because hash functions are *deterministic*). This way even if someone gets illicit access to the database, he will not know what are the original passwords and cannot do anything harmful with some hashes.

The left side of the slide features several light blue, hand-drawn style shapes on a dark blue background. These include a semi-circle at the top, a horizontal rounded rectangle below it, and a cluster of four rounded rectangles at the bottom, each tilted at a different angle.

Cryptography undoubtedly has a very important role in our contemporary technological world. Every enterprise system uses some of the methodologies that were described in the previous slides and we could not have reached this peak of digitalization without them. And there are a lot of theories about whether this is something good or bad but this is a totally different problem.

Unfortunately, cryptography has not helped us to develop one other aspect of our life – the art. I would not imagine someone to write a poem praising a hash function for example. Or a picture of any asymmetric-key algorithm.

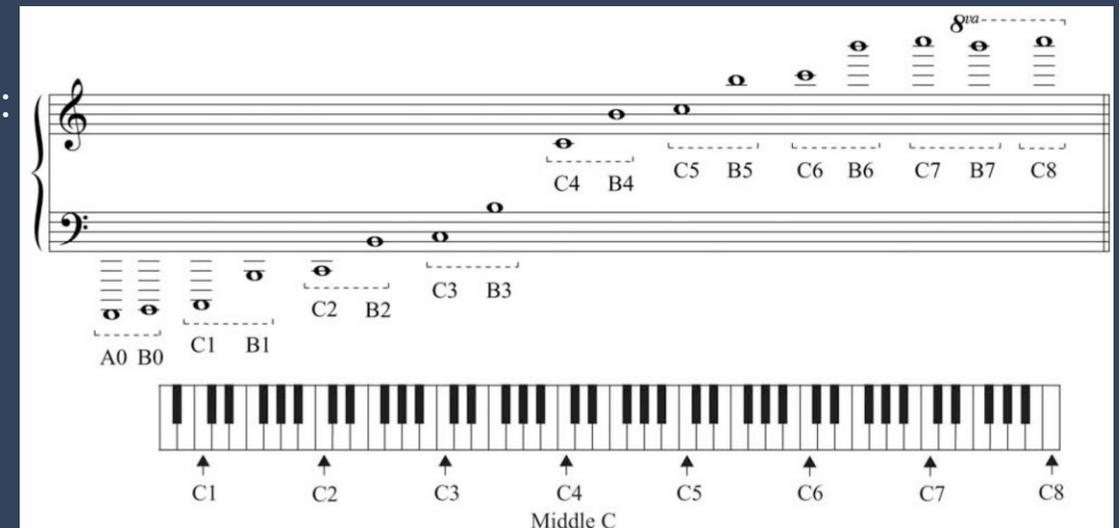
So... why do not we look at this from another perspective.

The first modern cryptographic algorithm using music in its core

- It was developed in 2010.
- It uses all letters from the English alphabet and all digits.
- It is a symmetric-key substitution algorithm and its key is the ordering of all symbols.

Before proceeding with the next slide, we should note some definitions from the music theory:

- There are seven note signatures defined as follows:
C, D, E, F, G, A, B
- An "octave" is a group of 12 semi-tones. From the perspective of physics, this is the interval between one tones and another with double its frequency. On this picture the intervals C1-B1, C2-B2, etc. Are examples for octaves



How it works?

Plain text: We depart tomorrow

Encoded tones: 3 -12 29 -12 9 2 -5 5 5 8 25 8 -5 -5 8 3

The symbols are ordered in some random way (according to the key). This is an example:

```
Symbol: 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 0 1 2 3 4 5 6 7 8 9
Index:  15 12 26 29 1 6 3 11 36 32 14 9 25 33 21 22 34 8 30 18 7 17 16 5 14 24 4 27 20 13 2 31 19 35 28 23
```

For each index (from 1 to 36) is assigned a unique tone described as its offset from "Middle C" - note that this algorithm uses three octaves.

```
Index: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
Tone: -12 -11 -10 -9 -8 -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
```

We encode a given plain text as for each character we substitute its value with a fraction number in the range $[-1, 1]$ that can be used to produce actual sound. It is computed by the following formula:

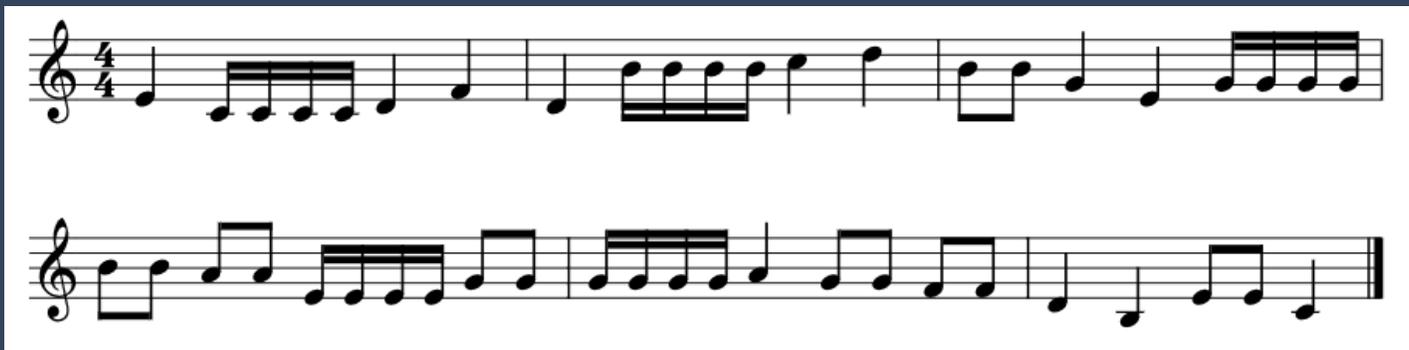
```
let x be the tone corresponding to the index of the current symbol.
tone_frequency = (2x - a - b) / (b - a), where a = -12, b = 23
tone_frequency = (2x - 11) / 35
```

It is apparent that we can revert these computations in order to decode a received message.

```
let y be the received fraction number representing the tone frequency.
tone = (y * (b - a) + a + b) / 2
tone = (y * 35 + 11) / 2
```

Another principle of music cryptography

- In 2016 another relatively simple principle was announced. In general - it is not an actual algorithm but an additional layer that can be applied to any other substitution algorithm.
- For each letter according to its frequency of usage, is assigned a tone and a beat division. And these tones are not randomly selected - they are defined by the circle of fifths.
- For example, the text "*It was a beautiful performance*" will produce the following music. And it actually is quite melodic for something randomly generated.

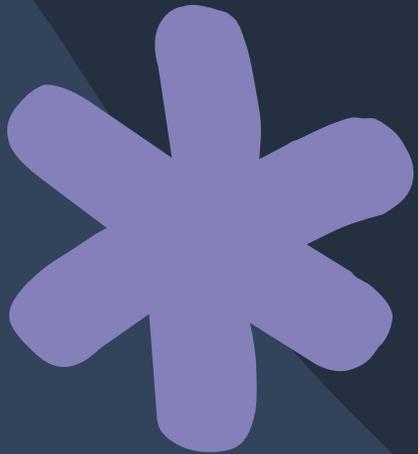


Letter	Tone	Beat division
e	C	100
t	G	100
a	D	100
o	A	100
i	E	100
n	B	100
s	F	100
h	C	50
r	G	50
d	D	50
l	A	50
c	E	50
u	B	50
m	F	50
w	C	25
f	G	25
g	D	25
y	A	25
p	E	25
b	B	25
v	F	25
k	C	33
j	G	33
x	D	33
q	A	33
z	E	33

Musical cryptography in the past

- Currently, the most popular techniques for musical cryptography are using symmetric-keys which means that they cannot be intergated as well as any assymmetric-key algorithm. Still this is a progress that should be used as a trampoline for further discoveries.
- In the past, nusical cryptography has been a very popular theme. Mathematicians and cryptologists such as John Wilkins and Philip Thicknesse have claimed that music cryptography is the best way of transporting secret messages because no one will ever suspect a melody to contain some encoded information. Music was perceived as a perfect camouflage and a very powerful steganographic tool.

The first ever systems of musical cryptography



- Philip Thicknesse also tried to give a musical representation of the famous steganographic cipher of the English philosopher Francis Bacon.
- Michael Hydn (the brother of Joseph Hydn) is author of another musical cipher dated from 1808 that is again a regular substitution cipher – each letter is represented as a separate tone. Olivier Messiaen is one of the modern musicians that tried something similar.
- There are also a lot of famous examples for musical cryptograms where the notes themselves represent the hidden message. For example, composers like Johann Sebastian Bach, Joseph Maurice Ravel, Claude Debussy, Olivier Messiaen and Dmitri Shostakovich even tried to spell their names using musical notation and different kind of motifs.