Cryptography's Application in Numbers Station

Jacqueline - 13512074[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13512074@std.stei.itb.ac.id

***Abstract*—Numbers station is a type of shortwave radio, categorized as an unusual broadcast. It is often built by artificially generated voices, which are letters, words, tunes, numbers, or Morse code. Numbers station, which is now used by spies to sending messages, is using cryptography--an application from number theory--in translating those messages.**

***Index Terms*—Cryptography, numbers station, shortwave radio, number theory.**

I. INTRODUCTION

Espionage is always interesting. Every single thing about it, either it comes in a novel, a movie, or in real. Cryptography is as well interesting.

People asked why the spies are still using numbers station for some ways to communicate the instructions. As now, many high technologies are so compromising. Why not using telephone, it is can dial internationally, after all.

The answer is about anonymity and Traffic Analysis. A spy, who--just say--disguised as a taxi driver would not seem suspicious when receiving message. Who knows it is an instruction from his agency--say FBI--that is being transmitted from faraway place.

Furthermore, if using telephone to sending instruction, it is could be tracked easily. It could be analyzed to give information, such as who is the sender and where, who is the receiver and where. Using it is really dangerous way more than communicate with regular basis.

Sending message using numbers station is so secure. It use cryptosystem called one-time pad (simple and strong symmetric cipher). The key that is used for encryption and decryption is string of random numbers (really random so no one could get it by seek for its pattern).

II. FUNDAMENTAL THEORIES

To know an application of cryptography in numbers station, let first know about what based the cryptography and the cryptography itself.

A. Number Theory

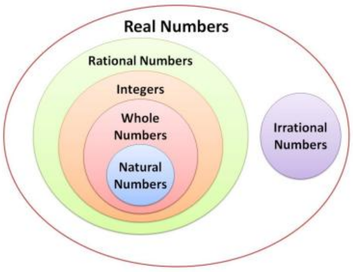


Fig. 1 Diagram of number

Number theory is a branch of pure mathematics. It studies prime numbers, the properties of objects made by integers (example: rational numbers) or generalized by integers (example: algebraic integers). Some of modern number theories are Fermat and Euler.

1. Fermat

Pierre de Fermat (1601-1665) discovered *Fermat's Little Theorem*, that says, if *a* is not divisible by a prime *p*, then $a^{p-1} \equiv 1 \pmod{p}$.

For every integer *a* we have $a^p \equiv a \pmod{p}$.

The lack is, there is a composite integer *n*, so $2^{n-1} \equiv 1 \pmod{n}$. It is called pseudoprime to the base 2.

2. Euler

Euler (1707-1783) made *Proofs for Fermat's statements*. Because in Fermat's lifetime, he almost published nothing, although he discovered things.

Number theory has many applications. Such as ISBN code, hash function, and cryptography.

ISBN code has 10 characters. Sometimes, being grouped with space or line (example: 0-3015-4561-9). There are four parts of the code:

1. Identification the language
2. Publisher's code
3. Unique code of that book
4. Character for test (number or letter X (=10)).

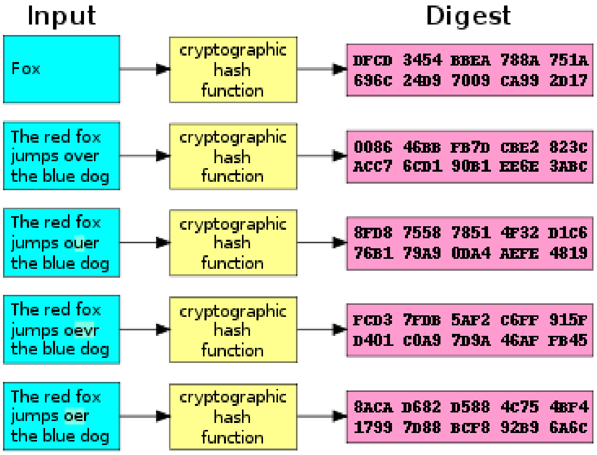

Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Fig. 2 Cryptographic hash function

Hash function is for addressing in memory.

$h(k)$ = mod m

- m: number of locations of memory that are available
- k: key (integer)
- $h(k)$: location of memory for record with k.

It will be made collision if hash function gives the same h for different k. If so, check the next empty element. This function can be used to locate the element that is searched also.

B. Cryptography

Cryptography is from two words, cryptology and graphein, from Greek. Cryptology (κρυπτός) means hidden and graphein is writing. This is a study of techniques for secure communication, in the presence of adversaries (third parties).

In any encryption system, the message to be sent is called plaintext. This message can be a text, picture, audio, or video. In some ways, it is encrypted to be ciphertext, then, being transmitted or saved in storage.

Usually, to be able to encrypt, needs a secret piece of information--called key--to scramble the message. On the other hand, when it comes to be decrypted, this key will be used to decrypt that ciphertext into plaintext.

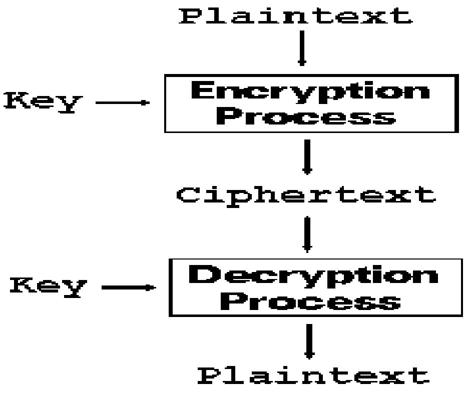


Fig. 3 The encryption and decryption flow

Usually, one or more cryptographic primitives are used to develop more complex algorithm. It is called cryptosystem (cryptographic system), designed to provide particular functionality while guaranteeing certain security properties. The examples of known cryptosystem are RSA encryption, El-Gamal encryption, and Schnorr signature.

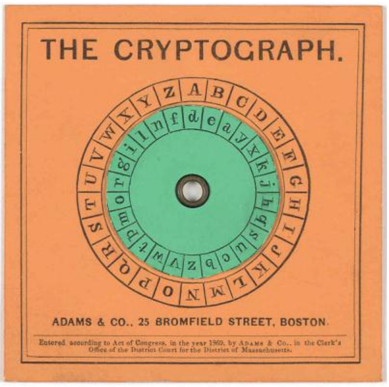


Fig. 4 The cryptograph. Boston: Adams and Co., 1869

There is a study about how to implement and integrate cryptography in best in software, called Cryptographic engineering and Security engineering.

C. Shortwave Radio

Shortwave radio is a radio communication that uses the upper medium frequency and all of the high frequency portion of radio spectrum (between 1,800-30,000 kHz).

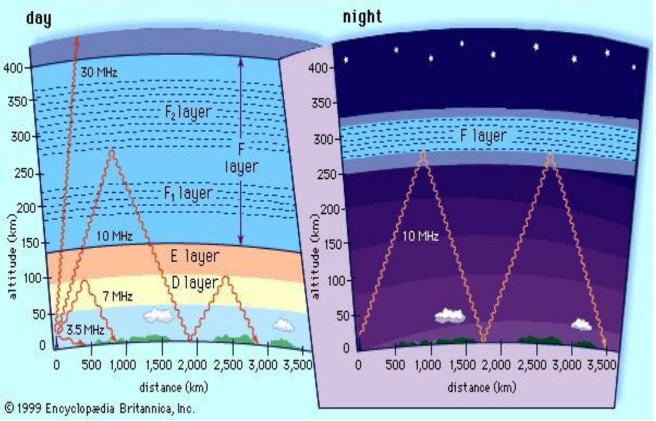


Fig. 5 Shortwave reflection off the ionosphere

It is used for long distance communication. Radio waves reflected from ionosphere back to Earth. So, allow communication around the curve of Earth. Used for broadcasting video or music, communication to ship or aircraft, or to remote areas out of reach.

Fig. 6 Digital shortwave receiver

Some of the advantages of using shortwave rather than new technologies are, it is difficult for program to censor it; useful for make authorities more simple in restrictive countries. Other advantages are, many countries continue to spreading the ownership of shortwave receivers widely, there is already available the shortwave portable receiver, also, shortwave travels farther than broadcasting by FM.

On the other hand, the disadvantages are, the broadcasts often disturbed by electrical interference, disturbances in atmosphere, and overcrowding wavebands. The shortwave radio depends on atmospheric conditions, so the best frequency for hearing can be different by the vary of time. It makes hard to be used by listeners who are not technically-minded.

D. Numbers Station

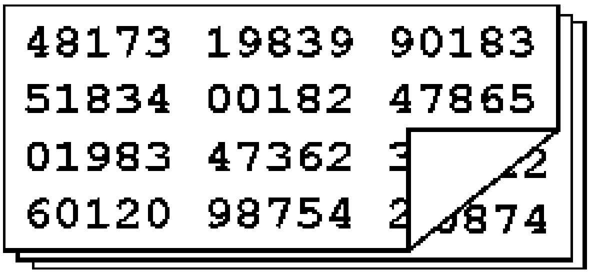
Fig. 7 Sketch of numbers station

Numbers station is broadcasted by radio, which appear in shortwave, for twenty four hours a day on many different frequencies. This is transmitting a message that really not for everyone to know. Usually used by secret agents in one agencies.

Numbers station has an introduction, for the start. It could be a single letter, key of Morse, or a piece of music. After that, there's a voice, in common language, begins saying numbers. These numbers are usually said in groups, one group about three or five digits. Sometimes, the group is repeated or even the whole message. Then, come an "end" by voice or repeated of the introduction music.

Fig. 8 Morse-Generator

To make that message "inside" the numbers station secure, do the encoding stage and use one-time pad to cipher the text. So, even it can be used to send messages to foreign country--because using shortwave radio--the "reader" is just will be the one who should read it.



48173 19839 90183
51834 00182 47865
01983 47362 3 2
60120 98754 2 874

Fig. 9 An example of one-time pad

It is still not clear when numbers station begins. What is known is, during the World War II, many countries were using it. Numbers station is so powerful. They allow anonymity of the receiver--can be anywhere and at any time without fear of detection.

Numbers station sends message that is already enciphered in form of groups (figures or letters) using one-time pad. On this pad, printed sets of random numbers. It is just the sender and the receiver who have this pad. Like its name, this thing just used once and then people who have it, destroy it.

Everyone can hear numbers station twenty four hours a day on the shortwave bands. The equipment that needed is any domestic shortwave radio with a whip antenna. It will allow to pick up numbers station. Sometimes, radio with the ability to receive USB and LSB transmissions will be useful (depends on what mode the message is transmitted). But, to be noted, in the United Kingdom, it is illegal to listen to these transmissions.

Now, numbers station has not seem to be left, because some countries even discover and design new languages station.

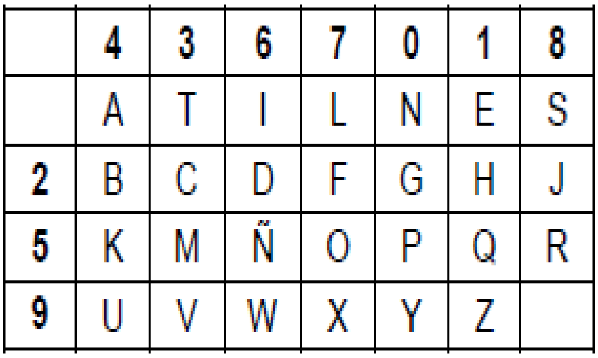
III. Cryptography in Numbers Station

As already said, numbers station is made to send and receive message securely. Here where cryptography takes place, by cipher it and decipher it.

Before it is broadcast, the operational message is encrypted into unintelligible series of numbers by using crypto algorithm. If one-time pad is properly used, the message would be unbreakable, except by the one this message for.

Before encryption, the message (plaintext) is converted into digits. One from many ways to do it is by using straddling checkerboard. This is the most common and cheapest method. This checkerboard is used to decrypt the message back into plaintext as well.

The example here use the checkerboard from the case about Ana Montes who was arrested in 2001. She was charged with espionage while working in US Defense Intelligence Agency.



	4	3	6	7	0	1	8
	A	T	I	L	N	E	S
2	B	C	D	F	G	H	J
5	K	M	Ñ	O	P	Q	R
9	U	V	W	X	Y	Z	

Fig. 10 Montes' Checkerboard

If we want to convert letter "A", read the digit at the top of the row. So, "A" = 4. For "G", because it is less frequented used, placed followed by column. Read the digit of the column, then its row. "G" is 20.

Let convert the simple message "SECRETO" into digits:

S E C R E T O
8 1 23 58 1 3 57

After that, use the one-time pad to encrypt it. The one-time pad is subtracted from the plaintext without borrowing (example: 3 - 5 = 13 - 5 = 8). The amount of digits in one-time pad has to be the same with ciphertext (plaintext as well).

```
Plaintext           81235 81357
One time-pad      - 20093 25848
                  -------------------
Ciphertext          61242 66519
```

Then, the ciphertext is broadcast by shortwave radio.

The one who receive it (by knowing the right frequency), write it down. Underneath that ciphertext, write the one-time pad. Adding them without carry (example: 9 + 6 = 5).

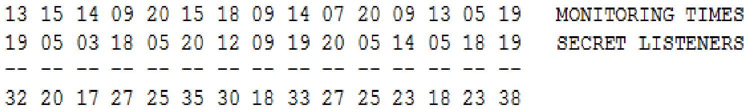
```
Ciphertext          61242 66519
One time-pad      + 20093 25848
                    -------------------
Plaintext           81235 81357
```

After that, use checkerboard to reconvert the digits into readable text. 81235 81357 -> SECRETO.

Another example in handling the message is shown below.

In here, each letter of alphabet is assigned by a number. Letter A has value 1, B = 2, C = 3, and so on until Z = 26.

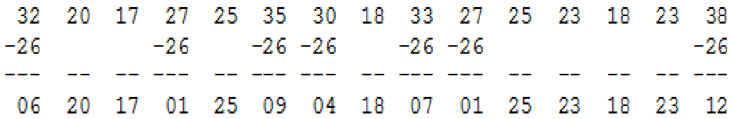
Then, add the plaintext number to the corresponding key number of each letter in the message.



```
13 15 14 09 20 15 18 09 14 07 20 09 13 05 19   MONITORING TIMES
19 05 03 18 05 20 12 09 19 20 05 14 05 18 19   SECRET LISTENERS
-- -- -- -- -- -- -- -- -- -- -- -- -- -- --
32 20 17 27 25 35 30 18 33 27 25 23 18 23 38
```

Fig. 11 Adding each plaintext to corresponding key number

Next, exceed 26 by subtracting that result with 26 and using the difference or is called taking the modulus (after reaching 26, "wrap around" and continue counting at 1).

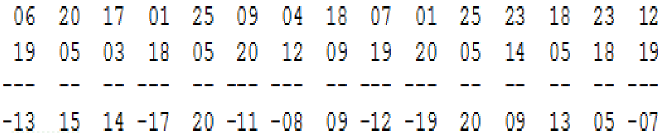


```
 32  20  17  27  25  35  30  18  33  27  25  23  18  23  38
-26         -26     -26 -26     -26 -26                 -26
---  --  -- ---  -- --- ---  -- --- ---  --  --  --  -- ---
 06  20  17  01  25  09  04  18  07  01  25  23  18  23  12
```

Fig. 12 Taking the addition result modulo 26

Get the encoded message: 06 20 17 01 25 09 04 18 07 01 25 23 18 23 12 (means FTQAYIDRGAYWRWL).

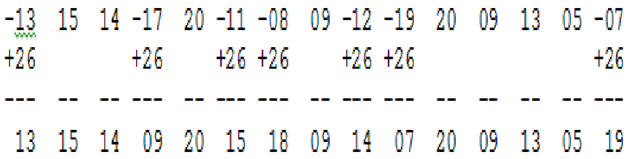
Now, when it is have to decrypted to plaintext, first, use the same one-time pad (consists identical key). Then, subtracting it with corresponding ciphertext letters.



```
 06  20  17  01  25  09  04  18  07  01  25  23  18  23  12
 19  05  03  18  05  20  12  09  19  20  05  14  05  18  19
---  --  -- ---  -- --- ---  -- --- ---  --  --  --  -- ---
-13  15  14 -17  20 -11 -08  09 -12 -19  20  09  13  05 -07
```

Fig. 13 Decoding the received message by subtracting

Now, to get the plaintext, add it with 26 (values that fall below 1 are “wrapped around”).



```
-13  15  14 -17  20 -11 -08  09 -12 -19  20  09  13  05 -07
+26         +26      +26 +26     +26 +26                  +26
---  --  -- ---  -- --- ---  -- --- ---  --  --  --  -- ---
 13  15  14  09  20  15  18  09  14  07  20  09  13  05  19
```

Fig. 14 Taking the difference modulo 26

So, it gives the plaintext message: MONITORING TIMES.

IV. Conclusion

There are so many applications from number theory. One of them is the well-known and delightful cryptography. Cryptography as well, can be used in many things. Numbers station, as one of it, giving so big opportunity, especially for the spy. Using crypto algorithm in cipher and decipher text, make it so secure. It makes that called “unbreakable code” is possible.

Numbers station is collide the used of cryptography and shortwave radio. That shortwave radio is for transmitting the message. It makes possible the message travels overseas. Even every people with equipment required could hear it. The cryptography which makes it still secured.

Beside the secure from being eavesdropped, other reason why numbers station is still exist is, its secure from other people to track.

V. Acknowledgment

To Allah SWT. who is really blesses the author and allow this paper to be done, thank You. The author also wants to thank her lecturers, Harlili and Rinaldi, for giving knowledge in Discrete Mathematics subject.

References

[1] AJ Menezes, PC van Oorschot, and SA Vanstone, *Handbook of Applied Cryptography*.

[2] Munir, Rinaldi. 2008. *Struktur Diskrit*. Bandung: Penerbit Intitut Teknologi Bandung.

[3] *Cuban Agent Communications* (paper based on FBI and court documents).

[4] *The Conet Project* (booklet), Irdial-Discs.

[5] http://www.decodesystems.com/mt/98oct/crypt.html.
Access on 13th December 2013.

[6] http://nowiunderstandmath.com/nium_distance_edu_course.html.
Access on 13th December 2013.

[7] http://skeptics.stackexchange.com/questions/5291/the-mystery-of-numbers-stations.
Access on 13th December 2013.

[8] http://www.britannica.com/EBchecked/media/3698.
Access on 13th December 2013.

[9] http://en.wikipedia.org/wiki/Cryptographic_hash_function.
Access on 13th December 2013.

[10] http://en.wikipedia.org/wiki/Cryptographic_hash_function.
Access on 13th December 2013.

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 17 Desember 2013

Jacqueline - 13512074