One unusual algebra of special ciphers

Kiyomitsu Horiuchi
Faculty of Science and Engineering,
Konan University
Okamoto, Higashinada, Kobe 658-8501, Japan
E-mail address: horiuchi@konan-u.ac.jp

The cryptography is a means to defend some secrets. It is necessary to endure enough for the attack. And, it is requested that the modern cryptography be efficient from a practical side. however, we amateurs play by the code in the hobby or the game. It is neither a military purpose nor a business purpose. Hence, we produced the cryptography of the code daring to disregard efficiency. We combined the methods of easy cryptography of the principle on which the professional did not look back so much. A considerably strong one can be made when thinking about the restriction of efficiency by removing. If it is possible, we want to try to transform it, and to find algebraic interest.

1 Stream cipher

The stream cipher is a cryptographic algorithm that processes the flow of data one by one. The block cipher is a cryptographic algorithm processed at each unit of a specific number of bits. The block cipher is practicably used than the stream cipher. However, we dare to treat the stream cipher. We treat the symmetrical cryptography that uses the same key because of the encryption and the decryption.

1.1 One-time-pad

There is the cryptography called "one time pad". It is mathematically safe. It can be used even when the quantum computer becomes normal. It is unconditionally secure and theoretically unbreakable. It uses true random numbers and the exclusive-OR. Even the amateur understands the principle very easily. The key is random numbers. But, random numbers of the same length as the sent sentence are necessary. A random number can be used only once. As random numbers are disposable, we consume a large amount of them. The delivery of the key is a big problem. Hence, one time pad is rarely used. We want to remodel it and to use it.

1.2 One-time-surd

We look for the substitute of true random numbers. It is used as the key of the cryptography. The professional might think that it should be pseudo-random number. However, we propose to use irrational numbers. Everyone knows the surd is a progression not repeated by the decimal expression. Let's make a sequence with numbers of each digit of a irrational number. The sender of the ciphertext chooses one surd, and sends it to the receiver of the cryptography. It is much easier than sending a row of very long random numbers. One surd becomes an infinite row. We should not use a famous number alone. We recommend to mix different kinds of numbers. There are innumerably equations that a surd becomes an answer. The sender of the ciphertext can send it by choosing the equation. It is possible to play considerably among friends who can share the knowledge of mathematics. But, strength of the cipher falls if true random numbers are not used. We amateurs think it ' s safe to replace irrational number with a completely new sequence every time. Even if the ciphertext and the plaintext sent ahead are known, a new surd is not surmisable.

1.3 One-time-approximation

In modern times, even ordinary computers will calculate thousands of digits. However, is it accurate? It doesn't care even by the approximate value either. If we calculate with exactly the same calculation formula on a computer of exactly the same specification, we do not mind being wrong. The sender and the receiver of the cryptography can share the same number. The row of the figure is different depending on the approximation method. This might be able to be used for the cryptography. My friend uses the same old software on the same personal computer as me. It is likely to fail when someone tries analyzing with an excellent super computer.

1.4 Problem

Is the surd suitably chosen suitable for the cryptography?
The sequence created by surd has bias. An extreme example is shown. Liouville number is a transcendental number. This is not suitable for the substitute of random number.

$$\sum_{k=1}^{\infty} 10^{-k!} = 0.11000100000000000000000010...$$

Even if you seem good in the digit of the start, what occurs on the way of the digit is not understood. There is seven ZERO consecutive "0000000" even in the π.

Let's try to improve one-time-surd by amateur's method and to increase strength.

2 Cryptography not paid attention to

Two of the cryptography that we amateurs like are enumerated. We want to use these two.

2.1 Book key cipher

There is a cryptography that uses the book as a key. In the 19th century, this was widely used. One book used as a key between the sender and receiver is decided. The sender send the message which of characters in the book to be read. For example, 'Open page 5 of the book, and read the 11th character that exists in the third line'. Of course, this cryptography will be broken if the book is known. If you use the same sentence as the key, the book is known. Assume you discard used parts.
A longer sentence book than the plaintext should be used as a key. My friend uses the traditional comic story telling of Japan. It is an experiment on whether it is possible to use it in the spoken word that uses the traditional comic story tellin It is possible if it makes it to the sentence of the type with the voice-recognition software. Experts worry that books with meaning are keys. They might think that it should be pseudo-random number. If you use random number table instead of books, it might be a very strong cryptography. It is a level of a military cryptography of the 20th century. Still, if the table of random numbers is not renewed, it is broken. After all, the solution is disposable of random numbers. It might not be for practical use even if theoretically becoming a cryptography that cannot be solved.

2.2 Insertable cipher

Insertable cipher has been known for a long time. It fun as a word game. Even if foreign matter is inserted between a word and a word, we can understand almost the meaning. For example,
"The supply of game for London is going steadily up. ···" means
"The game is up."
They have become important seed of detective stories sometimes. But, it is very weak as cipher. Let's break it more disjointedly. If you insert another character between a letter and a letter, it is somewhat confusing.
For example, "gtiahtmabeup" means "game".
This flies and reads two characters. "ḡtiāhtm̄abēup". This only placed the obstruct between the character and the character. This is not a word any longer. The key to the decipherment may be needed. There is a way to make Insertable cipher stronger. It crushes more. The character is shown by the code, and the foreign body is inserted. For example, let "g" be "**01100111**". Hrere, "0" or "1" of the suitable numbers are inserted. The inserted number is changed. "0**01**11**1**0**0**11**0**01**1**0**1**10**1**".
The progression was able to be done. No one understands that this progression is "g". Of course, the key to the decipherment is needed. Additionally, the message becomes long.

3 About the cipher and long sentences

There was a strong demand that it wants to shorten the message as much as possible in wireless telecommunications. In order to avoid noise and disturbance, short message is better than long sentences. Generally, it will please the receiver if the sender send the simple sentence. However, long sentences are often necessary to accurately convey complicated contents. It is disliked that sentences become longer when encrypting messages. Someone say that long sentences may be not suitable for spying activities. It doesn't become terrorists' profits. But we think that normal people can tolerate it. If very strong security can be obtained, long sentences should also be allowed. Please assume that there is a sentence you want to keep secret and saved it in memory with a length of 10 times. Still it will be negligible capacity compared to saving movies or animations. In modern times, even communication with considerable capacity can be made easy. We abandon old common sense.

4 Cryptography that uses three sequences of random numbers

We tried the improvement of the cryptography that used the book. We thought the role of the message and random numbers should be reversed. In the case of book key cipher, the receiver had the book "that is, the table of random numbers" beforehand. And the sender sent the message which of characters in the book to be read. In case of the new system, the receiver have the message which of characters in the table of random numbers to be read. This message is the key. And the sender send a table of random numbers. This table of random numbers can improve very much because it will send it later though it is not true random numbers. As a result, it became a strong cryptography. This indicated a strong insertable cipher and the same thing. In addition, if we add the method of one-time-pad, it is a super-strong cryptography. First of all, we make the super strong one. It is the cryptography that uses three sequences of random numbers. Afterwards, we make it easy to use. We omit a detailed specification and describe the outline.

4.1 Concrete example

How to make our cryptography is shown according to a concrete example. We use the decimal number to explain easily. We assume that the sender want to send the sentence "56719". The plaintext $\{p_n\}$ is "56719". Three random number sequences are assumed to be the following $\{a_n\}$, $\{b_n\}$ and $\{c_n\}$ $(c > 0)$. It is not essential though assumes $c > 0$ for the explanation.

$$\begin{aligned} \{a_n\} &: \ 50258242361708941976584932663598104535 76... \\ \{b_n\} &: \ 2277940295875495181784203116377985706151... \\ \{c_n\} &: \ 3926948539214178142882659314571431241267... \end{aligned}$$

First of all, progression $\{d_n\}$ is made by the way of one-time-pad. It is a modulo operation.
Let $d_n = p_n + a_n (\text{mod } 10)$.

$\{p_n\}\ :\ 56719$
$\{a_n\}\ :\ 5025824236...$
Hence,
$\{d_n\}\ :\ 06967$

The sequence of $\{b_n\}$ is divided into the block by each number of c_n.

$$\{b_n\}\ :\ \underbrace{227}_{3}\underbrace{794029587}_{9}\underbrace{54}_{2}\underbrace{951817}_{6}\underbrace{842031163}_{9}\underbrace{7798}_{4}...$$

And, we put d_n during the block one by one. This is ciphertext $\{e_n\}$.

$$\{e_n\}\ :\ 227\check{0}794029587\check{6}54\check{9}951817\check{6}842031163\check{7}7798...$$

If the receiver has sequences $\{a_n\}$ and $\{c_n\}$ as a key, it is possible that he deciphers the ciphertext $\{e_n\}$. The $\{c_n\}$ shows the number of characters not read. The $\{a_n\}$ is a key to one-time-pad. If three sequences $\{a_n\}$, $\{b_n\}$ and $\{c_n\}$ are disposable random numbers, this cryptography is surely strong. We used decimal number numbers to explain easily. You should actually process it by a binary number. In case of insertable cipher, the character can be shown by the code and the foreign body can be inserted. The amount of the foreign body increases further. However, $\{c_n\}$ should be a sequence including a big number. Sentences become long though it becomes safe when the number of $\{c_n\}$ is large. Hence, this should not be a binary number.

4.2 Strength of cryptography and our suggestion

If the first five figures of $\{a_n\}$ are 0, the ciphertext ahead is as follows.

$$\{e'_n\}\ :\ 227\check{5}794029587\check{6}54\check{7}951817\check{1}842031163\check{9}7798...$$

Even if "0" continue continuously, it is possible to use our cipher. The role as the ciphertext is played. Hence, we propose to use irrational numbers as $\{a_n\}$.

Moreover, if all $\{c_n\}$ is "1", the ciphertext is as follows.

$$\{e''_n\}\ :\ 2\check{5}2\check{6}7\check{7}7\check{1}9\check{9}4029587549518178420311637798...$$

When all of $\{c_n\}$ are adjusted to one, it is too easy. Still, this is a ciphertext because it is defended by $\{b_n\}$ that can be used. We want to admit $\{c_n\}$ to be made from irrational numbers. The $\{b_n\}$ is disposable random numbers though confirmed. This is a last redoubt. It is not necessary to send this beforehand. After all, we propose the cryptography by two disposable surd and one disposable random numbers sequence. We will call the cryptography "**one-time-2+1**".

The situation of "**one-time-2+1**" is summarized.
The $\{a_n\}$ and $\{b_n\}$ are keys.
They are generated from two surds.
It is necessary to pass them to the receiver without being known to the eavesdroppers.
It is possible to send them comparatively easily.
It is possible to exchange them frequently.
The $\{b_n\}$ is long random numbers sequence.
This is sent with the message. Every time, it is exchanged.

5 Unusual algebra on Cryptography

It is assumed that there are two numerical values preserved in Cloud by the ciphertext.

To keep it, we informed them of the ciphertext. However, we are not informing them of the numerical value. It is possible to preserve it by adding two numerical values, and encrypting the result. However, it is assumed that it is troublesome.
It is assumed that the custodian of Cloud exists. He doesn't know the numerical values. He doesn't know the key to the cryptography. He knows the ciphertext. Can we have him write the ciphertext of the numerical result?

There is a cryptography that this is possible. It was possible to make it by transforming "one-time-pad" a little. It is amateur's cryptography that changes exclusive-OR into a strange addition. Is it possible in our cryptography "**one-time-2+1**"? At first, we tried to limit the generation method of the cryptography, and to make the state to do an algebraic operation easily. However, we did not come satisfactorily though a considerable limitation was done. We can do modulo operation on the same digit But, it is difficult essentially to raise and to lower the digit. It has remained as a research topic. Should we think "Being not able to do this easily means this cryptography is not weak."?

There is another one proposal. It is dangerous for us to use the same sequences on $\{a_n\}$ or $\{c_n\}$. The preservation of the surd used in the past is also dangerous. We put up an appropriate label. And, the label is preserved. How is the label applied? It wants to prevent original being understood, and to distinguish. someone think about "hash function" at once. We think that it is insufficient. We assume that we have already used $\sqrt{2}$ for the seed of $\{a_n\}$. We do not want to use $1+\sqrt{2}$ and $0.001\sqrt{2}$, because the row of the same figure appears. However, we might use $7\sqrt{2}$. We are groping for the use of a strange algebraic system for such a check. This is a research topic when the future.

This paper is dedicated to my best friend Mr. Chikaharu Omoto who died suddenly in 2019.