# Digit addition process

This simple procedure can be seen already since the beginning of modern Cryptography. Unfortunately we have found so far, no such documents from the time of the ancient Greeks or Egyptians, but it is not excluded that these very intelligent people already knew this procedure.

## Based on

Perhaps it lies in the simplicity of the application. Because you need to control only the basic concepts of "computing".

For the successful use, knowledge of the numbers already ranges from "0 to 9".

Okay, is there a simple difficulty here.

You must apply a mathematical method, which is some getting used to.

Normally you expect

$$4 + 5 = 9 \text{ or } 6 + 6 = 12$$

We use the so-called modulo (10) - procedure for use with digit addition process.

And so is derived from the (mod 10) (4 + 5) = 9 but from mod(10) 6 + 6 = 2

Or mod(10) 5 + 5 = 0

But beware, this addition method makes no security, there is only a transformation rule.

Our correspondence is done by using letters and digits and other characters.

But also there a transformation rule, this is the substitution transformation.

For this transformation, there are a variety of rules have been developed on mathematical basis.

Some very interesting suggestions can find them in this regard by W.F.Friedman and the Cryptoanalyse materials.

## The substitution table

The substitution table is a necessity in the application of digit addition process. The cause lies in the discrepancy of the ranges of values.

In this procedure we have the numerals 0... 9 only. In contrast, includes the range of information from A to chiffrierenden...Z and 0..."9 and the characters;."+ - as well as space.

The number of required elements of the information exceed the amount of value stock of 0.. 9.

From this discrepancy, the introduction of a transformation table is required. This transformation tables are referred to as "Substitution table".

The creation of such tables is based on mathematical investigations.

The following examples, we fall back on an original substitution table that corresponds to the requirements of the German-speaking area.

| A<br>0 | S<br>1 | I<br>2 | N<br>3 | R<br>4 | **TAPIR VVS-ex. 03086** | | | | |
|---|---|---|---|---|---|---|---|---|---|
| (B)<br>50 | BE<br>51 | (C)<br>52 | CH<br>53 | (D)<br>54 | DE<br>55 | F<br>56 | G<br>57 | GE<br>58 | H<br>59 |
| (J)<br>60 | K<br>61 | L<br>62 | M<br>63 | O<br>64 | <br>65 | <br>66 | P<br>67 | Q<br>68 | S<br>69 |
| T<br>70 | TE<br>71 | U<br>72 | UN<br>73 | V<br>74 | <br>75 | W<br>76 | X<br>77 | Y<br>78 | Z<br>79 |
| WR<br>80 | BU<br>81 | Zi<br>82 | ZwR<br>83 | Code<br>84 | RPT<br>85 | <br>86 | <br>87 | <br>88 | .<br>89 |
| :<br>90 | ,<br>91 | -<br>92 | /<br>93 | (<br>94 | )<br>95 | +<br>96 | =<br>97 | "<br>98 | <br>99 |
| 0<br>00 | 1<br>11 | 2<br>22 | 3<br>33 | 4<br>44 | 5<br>55 | 6<br>66 | 7<br>77 | 8<br>88 | 9<br>99 |

When looking at this substitution table, they will find that all digits and characters through corresponding monograms or bi sociograms are defined.

So, the most common characters by monograms are defined. Other characters, or 2 - character strings are defined by two-digit bi sociograms.

There are also more functional character, as defined (ZWR) or the new row (WR), as well as the subsequent character structures between space by letters (BU) or digits (Zi), as well as short (RPT) for review.

The set elements are at the same time, such as; -/ () += "separately defined."

These definitions allowed a wide range of information to transkriptieren

On the picture you will find top-right classification.

We leave it with the theory and turn times to a practical example:

Take the to "Der Zauberlehrling von Goethe  1".

Original text

| BU | De | r | zwr | z | a | u | be | r | l |
|---|---|---|---|---|---|---|---|---|---|
| 81 | 54 | 4 | 83 | 79 | 0 | 72 | 51 | 4 | 62 |
| s | h | r | l | i | n | g | zwr | v | o |
| 1 | 59 | 4 | 62 | 2 | 3 | 57 | 83 | 74 | 64 |
| n | zwr | g | o | s | t | h | s | Zi | 1 |
| 3 | 83 | 57 | 64 | 1 | 70 | 59 | 1 | 82 | 11 |

Thus was created the following Zwischentext:

81544 83790 72514 62159 46223 57837 46438 35764 17059 18211

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 8154 4 | 8379 0 | 7251 4 | 6215 9 | 4622 3 | 5783 7 | 4643 8 | 3576 4 | 1705 9 | 1821 1 |

This Zwischentext consists only of digits in the range of 0.. 9.

## Enciphering

From the above generated Zwischentext a link to the key is carried out in the process of enciphering.

The key consists of a sequence of digits, with the values from 0... 9, which are randomly distributed.

This means that there is no functional link between the key components. This exclusion elements that have no mathematical functional dependency also applies to all groups of 2... n.

From this, the mathematical requirements of this very simple solution, learn but also secure solution.

Because they can, thus, CryptoLogic systems create, the a kryptologische strength of guaranteed, quasi convene up to absolute security, realize.

Because of the level of CryptoLogic security is determined by mathematical requirements.

Unfortunately not only is the problem, but, subsequent testing for compliance with the parameter with respect to the cryptographic strength of the used Schlüsselmittel.

Further details on this issue can be found under www.gocs.eu\pages\verschluess\deu\2-1.html

The art of creating a random sequence of digits, is the focus on the production and application of digit addition procedures.

Order not to be to this task, we take up published excerpts of these compilations also called worm tables back.

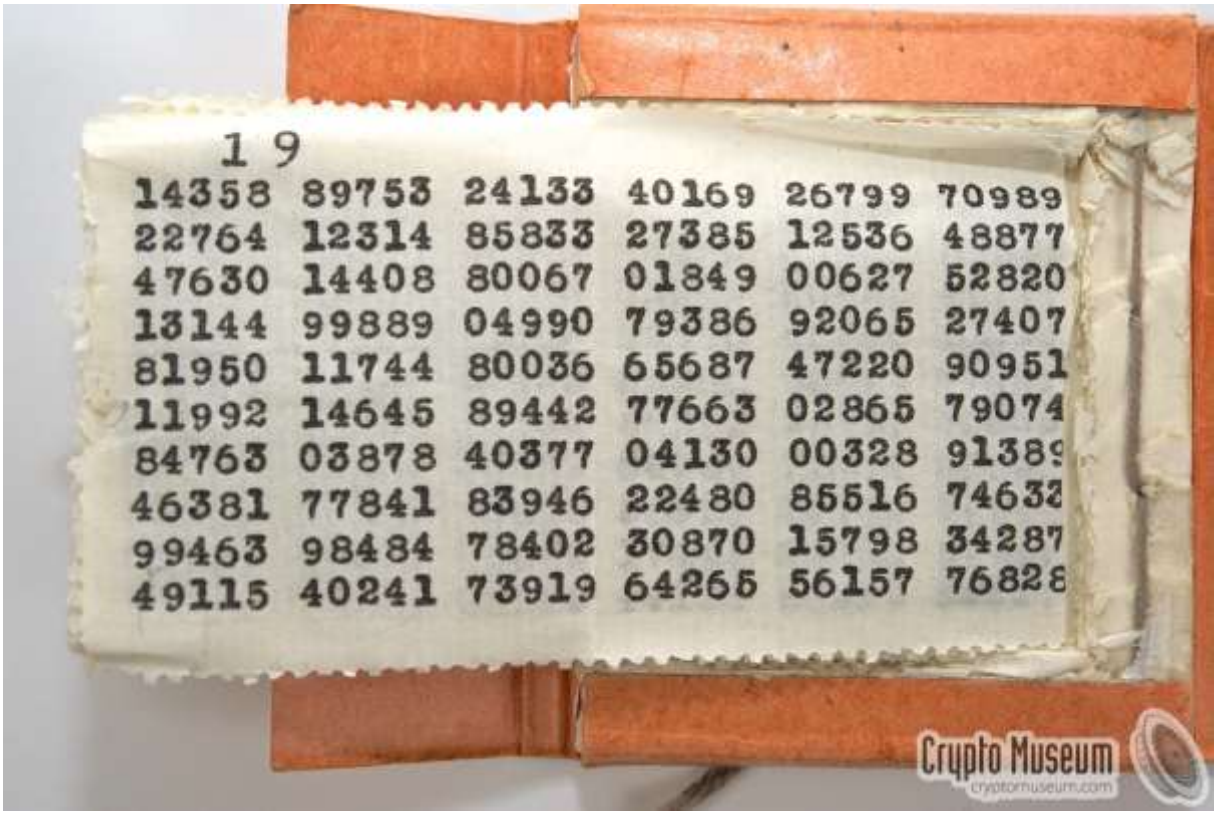
Here, we take back a publication published already on the Internet.

These designs to it you make it clear what is required for the security of information.

If you want to implement this in practice, they will realize what mathematical and technical apparatus is required to secure the information.

Therefore, we make it easy, we take a sequence of digits, we assume it meets the requirements for a random sequence of digits.

## Key table




'S comment:

The above paragraph 19 is used only to the Association for professional processing. She says the Dechiffreur, it was used the table 19 of the specification of key xxx.

This data is usually forward made the ciphertext.

Now, we want to encrypt the above text:

The Zwischentext is

81544 83790 72514 62159 46223 57837 46438 35764 17059 18211

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 81544 | 83790 | 72514 | 62159 | 46223 | 57837 | 46438 | 35764 | 17059 | 18211 |

The following five groups were taken from the ObigenSchlüsseltabelle:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 14358 | 89753 | 24133 | 40169 | 26799 | 70989 | 22764 | 12314 | 85883 | 27385 |

## Enciphering

The Zwischentext

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 81544 | 83790 | 72514 | 62159 | 46223 | 57837 | 46438 | 35764 | 17059 | 18211 |

The key text

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 14358 | 89753 | 24133 | 40169 | 26799 | 70989 | 22764 | 12314 | 85883 | 27385 |

Ciphertext = Zwischentext (mod 10) + key text

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 95892 | 62443 | 96647 | 02218 | 62912 | 27716 | 68192 | 47078 | 92832 | 35596 |

In the above table, it is generated cipher in the bottom line.

# Algorithm

Question: How is it made?

The algorithm will answer us this question.

Take on an item i of Zwischentextes and depending on an item i of the worm table.

i te E(Zwischentext) + i-th element (worm table) =(mod_10) i-te-Element(Geheimtext)

$GE_i$ ith secret text element

$ZwtE_i$ ith Zwischentext element

$SE_i$ ith key element

$GE_i$ (mod 10) $ZwtE_i$ = + $SE_i$

Consider this addition by the respective first element up to the last item in ascending order durchn.

The result is the following "cipher"

This term is somewhat misleading, because it is the text that is transmitted by all technical means open.

# Cipher

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 95892 | 62443 | 96647 | 02218 | 62912 | 27716 | 68192 | 47078 | 92832 | 35596 |

If they want to make the reverse process, decryption, now, as they dissolve this from bottom to top.