Method to encrypt numbers in binary system.

Juan Elías Millas Vera

juanmillaszgz@gmail.com

Zaragoza (Spain)

May 2020

0- Abstract:

This paper is an introduction to number cryptography. We use base-2 numerical systems and position properties to create a method which can convert numbers from binary to decimal and from decimal to binary in different ways depending of the integer used.

1- Introduction:

This idea arises from the study of binary and ternary number systems and in general of number systems other than decimal. The main function of the code is based on the characteristic that the basic binary system can be extended as required, using another positive integer instead of the number 2 as complement base but using just two digits.

2- Definition of the method:

A number n in decimal base can be encrypted in an extended binary system using an external semi-base k which always will be a positive integer. Following the next formula you will see the necessary exponents:

$$(1)\quad n_{10}=(\overbrace{a\dots a}^{k^n}\,\overbrace{a\dots a}^{\dots}\,\overbrace{a\dots a}^{k^2}\,\overbrace{a\dots a}^{k^1}\,\overbrace{a\dots a}^{k^0})_{(2\|k)}\qquad \forall\, a=0\vee 1\,\forall\, k,n\in\mathbb{N}$$

In this formula we can see that we use k^0, k^1, k^2,…,k^n depend which step of the semi-base k we need to encrypt the number.

It is very important to know that there will be a group with number t=k-1 digits of 0 or 1 in every step of the exponent of k:

$$(2)\quad n_{10}=(\overbrace{a\dots a}^{t}\,\overbrace{a\dots a}^{\dots}\,\overbrace{a\dots a}^{t}\,\overbrace{a\dots a}^{t}\,\overbrace{a\dots a}^{t})_{(2\|k)}\qquad \forall\, a=0\vee 1\,\forall\, k,t\in\mathbb{N}\quad \text{For } t=k-1$$

3- Examples of the method with different k:

3.1- k=2 (Traditional binary system)

- $0_{10}=0_{(2\|2)}=2^0\cdot 0$

- $1_{10}=1_{(2\|2)}=2^0\cdot 1$
- $2_{10}=10_{(2\|2)}=2^1\cdot 1+2^0\cdot 0$
- $3_{10}=11_{(2\|2)}=2^1\cdot 1+2^0\cdot 1$
- $4_{10}=100_{(2\|2)}=2^2\cdot 1+2^1\cdot 0+2^0\cdot 0$
- $5_{10}=101_{(2\|2)}=2^2\cdot 1+2^1\cdot 0+2^0\cdot 1$
- $6_{10}=110_{(2\|2)}=2^2\cdot 1+2^1\cdot 1+2^0\cdot 0$
- $7_{10}=111_{(2\|2)}=2^2\cdot 1+2^1\cdot 1+2^0\cdot 1$
- $8_{10}=1000_{(2\|2)}=2^3\cdot 1+2^2\cdot 0+2^1\cdot 0+2^0\cdot 0$
- $9_{10}=1001_{(2\|2)}=2^3\cdot 1+2^2\cdot 0+2^1\cdot 0+2^0\cdot 1$
- $10_{10}=1001_{(2\|2)}=2^3\cdot 1+2^2\cdot 0+2^1\cdot 1+2^0\cdot 0$
- …

3.2- k=3

- $0_{10}=00_{(2\|3)}=3^0\cdot 0+3^0\cdot 0$
- $1_{10}=10_{(2\|3)}=3^0\cdot 1+3^0\cdot 0$
- $2_{10}=11_{(2\|3)}=3^0\cdot 1+3^0\cdot 1$
- $3_{10}=1000_{(2\|3)}=3^1\cdot 1+3^1\cdot 0+3^0\cdot 0+3^0\cdot 0$
- $4_{10}=1010_{(2\|3)}=3^1\cdot 1+3^1\cdot 0+3^0\cdot 1+3^0\cdot 0$
- $5_{10}=1011_{(2\|3)}=3^1\cdot 1+3^1\cdot 0+3^0\cdot 1+3^0\cdot 1$
- $6_{10}=1100_{(2\|3)}=3^1\cdot 1+3^1\cdot 1+3^0\cdot 0+3^0\cdot 0$
- $7_{10}=1110_{(2\|3)}=3^1\cdot 1+3^1\cdot 1+3^0\cdot 1+3^0\cdot 0$
- $8_{10}=1111_{(2\|3)}=3^1\cdot 1+3^1\cdot 1+3^0\cdot 1+3^0\cdot 1$
- $9_{10}=100000_{(2\|3)}=3^2\cdot 1+3^2\cdot 0+3^1\cdot 0+3^1\cdot 0+3^0\cdot 0+3^0\cdot 0$
- $10_{10}=100010_{(2\|3)}=3^2\cdot 1+3^2\cdot 0+3^1\cdot 0+3^1\cdot 0+3^0\cdot 1+3^0\cdot 0$
- …

3.3- k=4

- $0_{10}=000_{(2\|4)}=4^0\cdot 0+4^0\cdot 0+4^0\cdot 0$
- $1_{10}=100_{(2\|4)}=4^0\cdot 1+4^0\cdot 0+4^0\cdot 0$
- $2_{10}=110_{(2\|4)}=4^0\cdot 1+4^0\cdot 1+4^0\cdot 0$
- $3_{10}=111_{(2\|4)}=4^0\cdot 1+4^0\cdot 1+4^0\cdot 1$
- $4_{10}=100000_{(2\|4)}=4^1\cdot 1+4^1\cdot 0+4^1\cdot 0+4^0\cdot 0+4^0\cdot 0+4^0\cdot 0$
- $5_{10}=100100_{(2\|4)}=4^1\cdot 1+4^1\cdot 0+4^1\cdot 0+4^0\cdot 1+4^0\cdot 0+4^0\cdot 0$
- $6_{10}=100110_{(2\|4)}=4^1\cdot 1+4^1\cdot 0+4^1\cdot 0+4^0\cdot 1+4^0\cdot 1+4^0\cdot 0$
- $7_{10}=100111_{(2\|4)}=4^1\cdot 1+4^1\cdot 0+4^1\cdot 0+4^0\cdot 1+4^0\cdot 1+4^0\cdot 1$
- $8_{10}=110000_{(2\|4)}=4^1\cdot 1+4^1\cdot 1+4^1\cdot 0+4^0\cdot 0+4^0\cdot 0+4^0\cdot 0$
- $9_{10}=110100_{(2\|4)}=4^1\cdot 1+4^1\cdot 1+4^1\cdot 0+4^0\cdot 1+4^0\cdot 0+4^0\cdot 0$
- $10_{10}=110110_{(2\|4)}=4^1\cdot 1+4^1\cdot 1+4^1\cdot 0+4^0\cdot 1+4^0\cdot 1+4^0\cdot 0$
- …

4- Conclusion:

In my opinion this could be a good method to encrypt numbers, that is because if you do not know the semi-base k you can not decrypt the binary number given.