# ASYMMETRIC ENCRYPTION / DECRYPTION WITH PENTOR AND ULTRA PENTOR OPERATORS

Artan Luma, Bujar Raufi, Xhemal Zenuni

Faculty of Contemporary Sciences and Technologies, South East European University
Ilindenska nn, 1200, Tetovo, Macedonia
{a.luma, b.raufi, xh.zenuni}@seeu.edu.mk

**Abstract:** Finding new approaches for asymmetric encryption / decryption process represents a milestone in cryptographic research and development. In this paper we introduce new algorithm for asymmetric encryption by utilizing two mathematical operators called Pentors and Ultra Pentors. The public and private key in this algorithm represent a quadruple of parameters which are directly dependent from the above mentioned operators.
The strength of the algorithm resides in the inability to find the respective Pentor and Ultra Pentor operator from the mentioned parameters.

**Keywords:** Asymmetric encryption, Asymmetric decryption, pentor

## Introduction

The introduction of public-key cryptography is often attributed to Diffie and Hellman, presented in ”new directions in cryptography” (Diffie & Hellman, 1998), where they described the usage of one way functions, and notions of trapdoor permutations in cryptography to which group belongs the public-key cryptosystem as well where there is a hidden trapdoor which enables the decryption to the legitimate party (Vaudenay, 2006).
A cryptosystem which is consisted of set of enciphering transformations $\{E_e\}$ and of deciphering transformations $\{D_g\}$ is called a public-key cryptosystem or an asymmetric cryptosystem if for each particular key pair $(e; d)$, the enciphering key $e$ is publicly available called the public key, whilst the deciphering key $d$, called the private key, is being kept secret. The mentioned cryptosystem must satisfy the fundamental property of infeasibility to compute *d* from *e* (Mollin, 2007).
In (Luma & Raufi, 2009) and (Luma & Raufi, 2010) we have introduced two new operators as mathematical models that can be used in cryptography
and in many other ideas as well. The contribution of this paper is that through these mathematical operators we are capable of creating and implementing powerful asymmetric encryption/decryption algorithm that can be utilized in many security systems such as banking systems, database security etc. We coin these two operators as Pentor and Ultra Pentor accordingly.

### Pentor Operator

We can introduce the Pentor of an integer number $n$ with base $B$. For every integer number $n$ there exists one Pentor for the given base $B$. For representing this operator mathematically, we are going to start from modular equation for Pentor of an integer number $n$ with base $B$ that fulfills the condition $\gcd(n, B) = 1$.
Considering the above mentioned conditions we could have:

$$B^m \cdot P(n) \equiv 1 (mod\ n) \qquad (1)$$

Where $B$ is the base of the integer number $n$, $P(n)$ is the Pentor for the integer number $n$ and $m$ represents the order of the Pentor $P(n)$ for the integer number $n$. The modular expression (1) can be also transformed to the equality expressions of the form:

$$B^m \cdot P(n) = 1 + n \cdot k \qquad (2)$$

$$P(n) = \frac{1 + n \cdot k}{B^m} \qquad (3)$$

where $k$ is an integer number that fulfils the condition for the fraction to remain an integer number. For example if we want to find the Pentor of the first order than, $m = 1$ the Pentor of the second order $m = 2$ and so on.

### Ultra Pentor Operator

The definition of Ultra Pentor of a number $n$ with base $B$ is that for every natural number $n$ there exist an Ultra Pentor operator for the given base $B$. The mathematical definition of an Ultra Pentor operator begins from modular equation of Ultra Pentor of integer number $n$ with base $B$ that satisfies the condition $gcd(n, B) = 1$. Considering the above mentioned conditions, the modular equation of Ultra Pentor is given as (Luma & Raufi, 2009):

$$B^m \equiv 1(mod\ n) \qquad (4)$$

where $m$ is an integer number. From the modular expression 4, a transformation to equality expression is possible by applying logarithmic operations on both sides and finding the Ultra Pentor given in the form as:

$$B^m \equiv\ 1\ +\ n\cdot\ l\,|\ \cdot\ log_B \qquad (5)$$

$$log_{B\ B^m}\ =\ log_B(1\ +\ n\cdot l) \qquad (6)$$

$$m\cdot log_B B\ =\ log_B(1\ +\ n\cdot l) \qquad (7)$$

where we will have :

$$m\ =\ log_B(1\ +\ n\cdot l) \qquad (8)$$

If $m\ =\ UP(n)$, then Ultra Pentor of integer number $n$ with base $B$ can be written as:

$$UP(n) =\ log_B(1\ +\ n\cdot l) \qquad (9)$$

In the above mentioned equation, $l$ is an integer number that fulfils the condition for $(1\ +\ n\cdot\ l)$ to be written as $B^a$, where $a$ is also an integer number. The rest of the work is organized as follows: In section 2 a mathematical outline of the new asymmetric encryption algorithm is being outlined. In section 3, a case study of the functioning of the proposed algorithm with an example is depicted and finally, section 4 concludes this paper with some future directions and proposals.

## New Asymmetric Encryption/Decryption Algorithm

Let us chose at the beginning a natural number $n$, from which we generate the Pentor and Ultra Pentor by using equations 3 and 9. Now, a prime number $p$ is chosen from which we find its primitive root and name it as $\alpha$.
Let us define a function $\gamma$ written as:

$$\gamma =\ n\cdot p\cdot UP(n) \qquad (10)$$

The resulted value from the function $\gamma$ is being checked by the number of digits it has and its digits are chopped" by the value of Ultra Pentor. All the "chopped pieces" are summed between each other and if the sequence is again longer than the value of Ultra Pentor the process is repeated until the sequence's length is less or equal to the value of Ultra Pentor. The digits of the produced sequence are right shifted by one place, resulting in non-repeating combination of sequences out of which we generate a block with length no greater than that of the value of Ultra Pentor.
Let us choose a value $a$ which represents one of the sequences taken from the above mentioned block. Now, we define a function $\beta$ written as:

$$\beta \equiv \alpha^a(mod\ p) \qquad (11)$$

After the above mentioned apparatus we define the public key as quadruples $(p, \alpha, \beta, P(n))$ while the secret key as $(n, UP(n), \gamma, a)$.
The overall process of communication through a secure line with above proposed approach goes as follows:

1) Adam sends to Eve the public key with quadruples $(p, \alpha, \beta, P(n))$.
2) Eve calculates a parameter:
$$r\ \equiv \alpha^{P(n)}(mod\ p)$$
3) Eve also calculates the ciphertext:
$$t\ \equiv\ \beta^{P(n)}m(mod\ p)$$
where $m$ is the message.
4) Now, Eve sends a pair $(r, t)$ to Adam.

5) Adam, after receives the pair $(r, t)$ by using its secret key finds the message as:

$$m \equiv t \cdot r^{-a} (mod\ p)$$

*Proof:*

$$t \cdot r^{-a} \equiv \beta^{P(n)} \cdot m \cdot (\alpha^{P(n)})^{-a} \equiv$$
$$\equiv (\alpha^{a})^{P(n)} \cdot m \cdot (\alpha^{-a})^{P(n)} \equiv$$
$$\equiv \alpha^{a \cdot P(n)} \cdot m \cdot \alpha^{-a \cdot P(n)} \equiv m\ (mod\ p)$$

## A Case Study

Let us illustrate the above stated algorithm through a real life example. Initially, let us adopt the value of $n = 13$. We find the value of $P(n)$ and $UP(n)$ as stated in equations 3 and 9 as follows:

$$P(13) = \frac{1 + 13 \cdot 3}{10} = 4$$
$$UP(13) = log_{10}(1 + 13 \cdot 76923) = 6$$

Now, if we adopt a prime number $p = 22621$ and by finding the primitive root of $p$ to be $\alpha = 2$, the $\gamma$ function, as seen from equation 10, can be calculated as:

$$\gamma = n \cdot p \cdot UP(n) = 13 \cdot 22621 \cdot 6 = 1764438$$

By taking the value of function $\gamma$ and by ”chopping” its digits from the right side by the value of $UP(n)$ which in our case is 6.

1 | 7 6 4 4 3 8

After we perform addition of these two blocks we get:

$$1 + 764438 = 764439$$

The non-repeating combination of the above presented value by doing a right shift as given in the algorithm above, results in a block as given below:

$$\begin{pmatrix} 7 & 6 & 4 & 4 & 3 & 9 \\ 6 & 4 & 4 & 3 & 9 & 7 \\ 4 & 4 & 3 & 9 & 7 & 6 \\ 4 & 3 & 9 & 7 & 6 & 4 \\ 3 & 9 & 7 & 6 & 4 & 4 \\ 9 & 7 & 6 & 4 & 4 & 3 \end{pmatrix}$$

By taking one of these combination and assigning to $a$, in a concrete case $a = 397644$ and calculating the function $\beta$ as given in equation 11 we will have:

$$\beta \equiv \alpha^{a} \equiv 2^{397644} \equiv 17011 (mod\ 22621)$$

If we return to the above elaborated steps of encryption/decryption with calculated values here, for a simple message like **”art”**, which has been converted to numbers based on letters from English alphabet (Luma & Zeqiri, 2008) the process will go as follows:

1) Adam sends to Eve the public key through quadruple $(22621, 2, 17011, 4)$.
2) Eve calculates a parameter:

$$r \equiv 2^{4} \equiv 16 (mod\ 22621)$$

3) Eve also calculates the ciphertext:

$$17011^{4} \cdot 11820 \equiv 588 (mod\ 22621),$$

where $m = 11820$ is the message.

4) Now, Eve sends a pair $(16, 588)$ to Adam.
5) Adam, after receives the pair $(16, 588)$ by using its secret key finds the message as:

$$m \equiv 588 \cdot 16^{397644} \equiv 11820 (mod\ 22621)$$

The strength of this algorithm consists in the secret key because of the parameter $a$ which is dependent from the function $\gamma$, while function  is dependent from the Ultra Pentor itself. If an intruder intersects the encrypted line, he does not possess the parameter $a$ which in our case, as explained in step 5 of our algorithm is a private key which only Eve possesses.

## Conclusion and Future Work

In this paper we have introduced new algorithm for asymmetric encryption / decryption by utilizing two mathematical operators called Pentors and Ultra Pentors. The strength of the proposed algorithm lies in the quadruples of parameters used as public as well as private keys.

Future work and development would involve the creation of electronic certificate which can be used in many aspects of everyday life such as: e-commerce, banking transactions, electronic signatures etc.

## References

Diffie, W, & Hellman, M (1998). New directions in cryptography. *IEEE Transactions on Information Theory*,

Luma, A, & Raufi, B (2009). New data encryption algorithm and its implementation for online user authentication. *Security and Management*, 81-85.

Luma, A, & Raufi, B (2010). Relationship between fibonacci and lucas sequences and their application in symmetric cryptosystems.*4th International Conference on Circuits, Systems and Signals*, 146-150.

Luma, A, & Zeqiri, N (2008). Data encryption using an algorithms implemented in RSA algorithm. *International Conference in Information Systems Security*, 146-149.

Mollin, R.A (2007). *An Introduction To Cryptography*. Chapmann & Hall.

Vaudenay, S (2006). *Classical introduction to cryptography: Applications for Communications Security*. Springer Science & Business Media, Inc.