ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 215–220
ISSN 1930-1235: (2008)

A NEW ENCRYPTION AND SIGNING ALGORITHM.

Urszula Romaczuk

John Paul II Catholic University of Lublin,
Lublin, Poland
urszula_romanczuk@o2.pl

Abstract. In this paper we describe a new method of encryption that originates from the public key cryptography and number theory. Our algorithm was inspired by the RSA algorithm and Diffie-Hellman key exchange protocol. It is based on a computationally difficult problem - the discrete logarithm problem in multiplicative group.

1. Basic idea

Let $\mathbb{A}$ and $\mathbb{B}$ be users that communicate in a secure channel based on public key cryptography. $\mathbb{A}$ is a sender and $\mathbb{B}$ is a receiver of a message. Hence, each of them have a pair of keys - public and private. $\mathbb{A}$ has pair $(k_{\mathbb{A}},\ l_{\mathbb{A}})$, $\mathbb{B}$ has $(k_{\mathbb{B}},\ l_{\mathbb{B}})$ ($k_{\mathbb{A}},\ k_{\mathbb{B}}$ are private keys and $l_{\mathbb{A}},\ l_{\mathbb{B}}$ are public keys). Assume that $\mathbb{A}$ wants to send c (that is encrypted message m) to $\mathbb{B}$.

Let f denote the encryption function and let f^{-1} denote the corresponding decryption function. In asymmetrical cryptography arguments of the function f are: receiver's public key $l_{\mathbb{B}}$ and plain text m, that is

$$c = f(m, l_{\mathbb{B}}),$$

where c is ciphertext. The decryption function's f^{-1} arguments are: the receiver's private key $k_{\mathbb{B}}$ and ciphertext c. In our case:

$$f^{-1}(c, k_{\mathbb{B}}) = m.$$

In this paper a different approach is presented. Namely, arguments of the encryption function are: plaintext m, the receiver's public key $l_{\mathbb{B}}$ and the sender's private key $k_{\mathbb{A}}$. Hence

$$c = f(m, l_{\mathbb{B}}, k_{\mathbb{A}}).$$

Similarly, arguments of decryption function f^{-1} are three parameters, that is: ciphertext c, receiver's private key $k_{\mathbb{B}}$ and sender's public key $l_{\mathbb{A}}$. We have

$$f^{-1}(c, k_{\mathbb{B}}, l_{\mathbb{A}}) = m.$$

This cross-keyed approach in both encryption and decryption functions aims not only at encrypting and decrypting, but also at signing, simultaneously. That makes receiver $\mathbb{A}$ ensured that $\mathbb{B}$ is an authentic sender of a message. Then, the sender cannot deny his authorship of a message, that is the authentication of the sender and typical digital signature take place at the same time. Hence, that signature

identifies the author of the message and checks that the message was not changed during transmission.

From a mathematical point of view I find this cryptosystem very interesting. It may be used e.g. to protect transmission in LAN networks.

2. Description of encryption and digital signature algorithm.

In this paper I assume that the reader has basic knowledge in abstract algebra and number theory.

Let $\mathbb{Z}_n$ denote the additive group of integers residues modulo n and let $\mathbb{Z}_n^*$ denote the multiplicative group of integers residues modulo n, where n is a natural integer. Let φ be Euler's function, that is, if m is a natural integer then $\varphi(m)$ denotes the number of integers that are less than m and relatively prime to m.

Lets assume $\mathbb{A}$ and $\mathbb{B}$ are going to communicate. First, each of them has to generate a pair of keys: public and private. Now they are ready to send each other a secret message.

Let $(k_{\mathbb{A}},l_{\mathbb{A}})$ be the pair of keys that belong to user $\mathbb{A}$. Similarly, let the pair $(k_{\mathbb{B}},l_{\mathbb{B}})$ belong to user $\mathbb{B}$.

1.: Keys generation.

1.1.: Both users set:

- two positive integers q and n, where q is prime. It is important to choose such integers that the discrete logarithm problem in $\mathbb{Z}^*_{\varphi(q^n)}$ is computationally difficult,

- integer $g \in \mathbb{Z}^*_{\varphi(q^n)}$ has such a property that it generates the biggest subgroup of multiplicative group $\mathbb{Z}^*_{\varphi(q^n)}$. It would be best if g generates the entire group $\mathbb{Z}^*_{\varphi(q^n)}$, so that the group would be cyclic. Of course:

$$\gcd(g, \varphi(q^n)) = 1 \quad \text{and} \quad g \neq 1.$$

Function $\gcd(n, m)$ denotes the greatest common divisor of integers n and m.

1.2.: Next, user $\mathbb{A}$ chooses randomly $x \in \mathbb{Z}^*_{\varphi(\varphi(q^n))}$, user $\mathbb{B}$ chooses $y \in \mathbb{Z}^*_{\varphi(\varphi(q^n))}$ and they compute $g^x,\ g^y$ modulo $\varphi(q^n)$. If

$$g^x \equiv 1 \,(\text{mod } \varphi(q^n)), \quad \text{or} \quad g^y \equiv 1 \,(\text{mod } \varphi(q^n)),$$

then x or y must be chosen randomly again. Clearly, $\varphi(q^n) = q^{n-1}(q-1)$.

1.3.: Both users agree on a hash function h which is used to generate a digital signature.

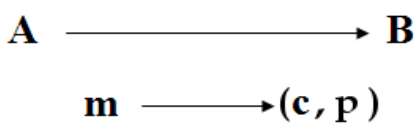
Then, for user $\mathbb{A}$:

- private key is $k_{\mathbb{A}} = x$,

- public key $l_{\mathbb{A}} = (\ g^x,\ q,\ n,\ h\ )$.

(User B: $k_{\mathbb{B}} = y$, $l_{\mathbb{B}} = (\ g^y,\ q,\ n,\ h\ )$).

Let $m \in \mathbb{Z}^*_{q^n}$. Lets assume that user $\mathbb{A}$ is going to send message m to user $\mathbb{B}$. Moreover, m is both encrypted and signed, so $\mathbb{B}$ receives (c, p), where c denotes ciphertext and p denotes the signature of that ciphertext.



Communication schema between users $\mathbb{A}$ and $\mathbb{B}$.

2.: **Encryption and signature.** (User $\mathbb{A}$).

2.1.: Gets public key of user $\mathbb{B}$, $l_{\mathbb{B}} = (\, g^y, q, n, h\,)$ and computes:

$$k \equiv (g^y)^x \equiv g^{xy} \,(\mathrm{mod}\ \varphi\,(q^n))\,.$$

2.2.: Next, he encrypts message m:

$$m^k \equiv c \,(\mathrm{mod}\ q^n)\,.$$

2.3.: Generation of signature p is as follows. Firstly:

$$r \equiv c^k \,(\mathrm{mod}\ q^n)\,.$$

Secondly, using hash function h, he computes signature $p = h\,(r)$.

2.4.: Ciphertext c and signature p is sent to user $\mathbb{B}$.

3.: **Decryption and verification.** (User $\mathbb{B}$).

3.1.: After receiving ciphertext $c\,'$ and signature $p\,'$ from user $\mathbb{A}$, he gets the public key of user $\mathbb{A}$ $l_{\mathbb{A}} = (\, g^x, q, n, h\,)$. Next he computes k and k^{-1}:

$$k \equiv (g^x)^y \equiv (g^{xy}) \,(\mathrm{mod}\ \varphi\,(q^n))\,,$$

$$k^{-1} \equiv (g^{xy})^{-1} \,(\mathrm{mod}\ \varphi\,(q^n))\,.$$

3.2.: In the next step $\mathbb{B}$ computes :

$$r\,' \equiv (c\,')^k \,(\mathrm{mod}\ q^n)\,.$$

3.3.: By using hash function h he gets p', so $p' = h\,(r\,')$. Next he checks that no enemy pretends to be the valid sender, that is, the following equation must occur:

$$p\,' = p\,''.$$

If so, that means nobody faked the ciphertext c', hence $c = c'$. Additionally, authentication of user $\mathbb{A}$ takes place at this moment, because the only persons that can compute k are $\mathbb{A}$ and $\mathbb{B}$. Now $\mathbb{B}$ is ready to process decryption of ciphertext c.

3.4.: Decryption of ciphertext c is as follows:

$$c^{k^{-1}} \equiv m \,(\mathrm{mod}\ q^n)\,.$$

and that is all.

Notice that the existence of the of inverse of the element g^{xy} in group $\mathbb{Z}^*_{\varphi(q^n)}$ is a sufficient condition of verification. Let us assume that such an $(g^{xy})^{-1}$ exists in that group. Then we have

$$c^{k^{-1}} \equiv \left[m^{g^{xy}}\right]^{(g^{xy})^{-1}} \equiv m^{g^{xy} g^{-xy}} \equiv m \,(\mathrm{mod}\ q^n)\,.$$

In fact, now it is sufficient to prove that the element $(g^{xy})^{-1}$ exists in group $\mathbb{Z}^*_{\varphi(q^n)}$.

By assumption $g \in \mathbb{Z}^*_{q^{n-1}}$. Moreover it is the generator of that group. Hence $g \in \left(1, g^{n-1}\right)$ and $\gcd(g, \varphi(q^n)) = 1$, so element g belongs to the multiplicative group $\mathbb{Z}^*_{\varphi(q^n)}$ and has its inverse. We have

$$1 \equiv g \cdot g^{-1} \equiv \left(g \cdot g^{-1}\right)^{xy} \equiv g^{xy} \cdot g^{-xy} \pmod{\varphi(q^n)}.$$

We proved that an inverse to the element g^{xy} exists in group $\mathbb{Z}^*_{\varphi(q^n)}$ Hence decryption is correct.

The strength of the described algorithm lies in the fact that having public keys of the sender and the receiver there is no possibility that an enemy gets the private key of neither sender nor receiver.

Indeed, we know public keys of users $\mathbb{A}$ and $\mathbb{B}$ because they publish their keys in public: $l_{\mathbb{A}} = (g^x, q, n, h)$ and $l_{\mathbb{B}} = (g^y, q, n, h)$. An enemy has no possibility of computing the private key of $\mathbb{A}$: $k_{\mathbb{A}} = x$. The element $g^x \in \mathbb{Z}^*_{\varphi(q^n)}$, $\varphi(q^n) = q^{n-1} \cdot (q-1)$ (as it's easy to prove). However, even if a generator g of a subgroup of the group $\mathbb{Z}^*_{\varphi(q^n)}$ was published publicly, the expression x would be based on a computationally hard problem, that is on discrete logarithm problem. Of course, we have to carefully choose a prime q and a natural integer n. Hence, an enemy not only has to compute private keys of sender and receiver, but additionally he has to guess the generator g that was used in encryption.

Notice that if an enemy catches both ciphertext and signature (c, p), which was sent by user $\mathbb{A}$ to $\mathbb{B}$, then he also knows public keys : $l_{\mathbb{A}} = (g^x, q, n, h)$ and $l_{\mathbb{B}} = (g^y, q, n, h)$. However, he does not know the generator g of a subgroup of the group $\mathbb{Z}^*_{\varphi(q^n)}$ and private keys of $\mathbb{A}$ and $\mathbb{B}$, recpectively $k_{\mathbb{A}} = x$ and $k_{\mathbb{B}} = y$. It is clear that $x, y \in \mathbb{Z}^*_{\varphi(\varphi(q^n))}$, $\varphi(\varphi(q^n)) = q^{n-2} \cdot (q-1) \cdot \varphi(q-1)$. Of course, having this information, somebody can try brute force attack and check in turn every element of $\mathbb{Z}^*_{\varphi(\varphi(q^n))}$, but, as we know, if we choose a group of big enough order, then finding x to compute k, that is.

$$k \equiv (g^x)^y \equiv (g^{xy}) \pmod{\varphi(q^n)},$$

takes a large amount of time, up to a dozen or so years. Additionally k^{-1} must also be found to decrypt the ciphertext c.

3. Conclusion.

In choosing an adequate multiplicative group $\mathbb{Z}^*_{q^n}$, where q is prime and n is natural integer, it is important for the group $\mathbb{Z}^*_{\varphi(q^n)}$ to be cyclic. This guarantees that the ciphertext set extends to the maximum and the number of constant elements is minimal and equal 2 (that is elements where $f(m) = m$, where f is an encryption function and $m \in \mathbb{Z}^*_{q^n}$, these elements are $m = 1$ and $m = q^n - 1$, because $2 | \#\mathbb{Z}^*_{q^n}$, where $\#\mathbb{Z}^*_{q^n} = (q-1)\, q^{n-1}$ is rank of a group $\mathbb{Z}^*_{q^n}$). This is indeed so, because the Abelian group $\mathbb{G}$ of rank n is a cyclic group, if and only if for any divisor d of n, there are exactly d elements fulfilling the condition $x^d = e$, where e is a natural element of the group.(See: [1])

After conducting research on multiplicative groups $\mathbb{Z}^*_{q^n}$ of residues modulo q^n, where q is prime and n is natural integer such as $n > 1$, I came to the conclusion that the most effective multiplicative group in the described method of encryption is $\mathbb{Z}^*_{3^n}$, that is, when $q = 3$. This is so, because group $\mathbb{Z}^*_{\varphi(3^n)} = \mathbb{Z}^*_{2 \cdot 3^{n-1}}$ is cyclic, that is, a generator g exists, which generates the entire group $\mathbb{Z}^*_{\varphi(3^n)}$ and not only

its subgroup and, as well, group $\mathbb{Z}^*_{\varphi(\varphi(3^n))} = \mathbb{Z}^*_{2\cdot 3^{n-2}}$ is cyclic, that is, a generator g' exists, which generates the entire group $\mathbb{Z}^*_{\varphi(\varphi(3^n))}$ and not only its subgroup. This means that the set of possible private and public keys extends to maximum size, that is $x, y \in \mathbb{Z}^*_{\varphi(\varphi(3^n))}$ and $g^x, g^y \in \mathbb{Z}^*_{\varphi(3^n)}$.

Indeed this is so because the following fact occurs: if p is an odd prime, for any natural integer n, the multiplicative groups $\mathbb{Z}^*_{p^n}$ and $\mathbb{Z}^*_{2p^n}$ are cyclic groups.(See: [2], [3])

After my research on groups of the form $\mathbb{Z}^*_{q^n}$, $n > 1$, I noticed that if we take a prime $q \neq 3$ and we apply it to the encryption algorithm, then there exist many fixed points. That means that there exists message $m \in \mathbb{Z}^*_{q^n}$, which stays unchanged after encryption, that is $c = m$. For $\mathbb{Z}^*_{3^n}$ we don't have that problem, because then every message $m \neq 1$ and $m \neq (3^n - 1)$ after encryption is different from ciphertext c. It is indeed so, because, in my opinion, the following hypothesis, which stems from my research, is true: the group $\mathbb{Z}^*_{\varphi(q^n)}$, $n > 1$ and for odd prime q is cyclic if and only if is odd prime $q = 3$. It was Professor Thomas Bier who reassured me that the above mentioned hypothesis is correct by proving this fact.

So far, I haven't come across any evidence in literature, which could prove that in the group $\mathbb{Z}^*_{3^n}$ or $\mathbb{Z}^*_{2\cdot 3^{n-1}}$, the discrete logarithm problem is computationally simple. Thus, it would be an interesting open problem to find such an algorithm, which would solve the problem of the discrete logarithm in the groups $\mathbb{Z}^*_{3^n}$ and $\mathbb{Z}^*_{2\cdot 3^n}$ for large values of n, given that such a discovery is possible today.

According to one theory, the discrete logarithm in the group $\mathbb{Z}^*_n$ when n has small prime factors is not a computationally difficult problem and is easy to solve. Regardless, there is no know algorithm for breaking the discrete logarithm in the proposed group $\mathbb{Z}^*_{3^n}$ or $\mathbb{Z}^*_{2\cdot 3^{n-1}}$ for sufficiently large n, though in the above mentioned group we have small prime factors.

When $n = 1$, we have a multiplicative group $\mathbb{Z}^*_q$ of residues modulo q. As we know, the multiplicative group $\mathbb{Z}^*_{\varphi(q)}$ is not cyclic for every prime number. However, when e.g. the prime number q is in the form $q = 2p + 1$ where p is a large Sophie Germain prime, then $\mathbb{Z}^*_{\varphi(q)} = \mathbb{Z}^*_{2p}$ is cyclic. Keep in mind that: a prime p is a *Sophie Germain prime* if both p and $2p + 1$ are prime. We do not yet know if an infinite number of Sophie Germain primes exist.(See: [5])

Continuing with this argumentation, if the prime number is in the form $q = 2p^m + 1$ where m is a natural integer and p is an odd prime number, then it becomes obvious that, in this case, $\mathbb{Z}^*_{\varphi(q)} = \mathbb{Z}^*_{2p^m}$ is cyclic (numbers in the form $q = 2p^n + 1$ where p is an odd prime and m is a natural integer do indeed exist, for example $163 = 2 \cdot 3^4 + 1$, $251 = 2 \cdot 5^3 + 1$, $487 = 2 \cdot 3^5 + 1$, $2663 = 2 \cdot 11^3 + 1$). I do not know how many such numbers $q = 2p^n + 1$ exist nor could I find any forms of such numbers in published literature. As far as I know $q = 2p^n + 1$ is not a prime number for every prime p and natural integer m. Let us say that a prime power p^e is called a *Sophie Germain prime power* iff p is odd and $q = 2p^e + 1$ is also a prime number, or if $p = 2$ and $e = 0, 1$.

Hence, the as yet unanswered question arises: for which other prime numbers q will the group $\mathbb{Z}^*_{\varphi(q)}$ be cyclic. I would be very interested in getting familiar with other suggestions regarding this open problem and the method of encryption proposed.

Attaching a signature is necessary to detect if somebody else pretends to be the sender of the message. Notice that determination of k which is used in encryption and decryption, can be done easily and independently only by sender and receiver.

If somebody wants to fabricate ciphertext and signature, he must know k and this leads to knowledge of the private key of the sender or the receiver. In such a situation the discrete logarithm problem must be solved, which is a computationally difficult problem.

The algorithm is based on the RSA encryption algorithm, the Diffie-Hellman key exchange protocol.

Acknowledgments: I would like to express my deepest gratitude to Professor Vasyl Ustymenko and Professor Thomas Bier for their guidance and kindness, as well as their helpful advice and valuable suggestions. In would like to particularly thank Professor Jerzy Urbanowicz for inspiration and encouragement, without which this cryptosystem wouldn't have come into existence.

References

1. Bagiski Czesaw ,,Introdution to group theory", SCRIPT, Warsaw 2002
2. Ireland Kenneth, Rosen Michael, ,,A Classical Introduction to Modern Number Theory", Springer, New York 1988
3. Leveque William Judson ,,Fundamentals of Number Theory", Addison-Wesley Publishing Company, 1977
4. Schneier Bruce ,,Applied Cryptography", WNT, Warsaw 1995.
5. Ribenboim Paulo ,,The Little Book of Big Primes", Springer-Verlag, New York Berlin Heidelberg 1991
6. Urbanowicz Jerzy Eugeniusz ,,Asymmetrical cryptography" - undergraduate lecture for IV/V - year students of mathematics at KUL in 2005/2006.