University of Business and Technology in Kosovo

UBT Knowledge Center

UBT International Conference

2018 UBT International Conference

Oct 27th, 3:15 PM - 4:45 PM

Use composite commutation functions in determining the Diffie-Hellman keys

Faton Kabashi

University for Business and Technology, faton.kabashi@ubt-uni.net

Azir Jusufi

University for Business and Technology, azir.jusufi@ubt-uni.net

Use of composite commutation functions in determining the Diffie-Hellman keys

Faton Kabashi[1] and Azir Jusufi[2]

[1,2] UBT – Higher Education Institution, Lagjja Kalabria, 10000 p.n., Prishtine, Kosovo

[1]faton.kabashi@ubt-uni.net, [2]azir.jusufi@ubt-uni.net

Abstract. The Diffie-Hellman protocol was proposed by Whitfield and Martin Hellman. Diffie and Hellman wanted a mathematical function where encryption and decryption would not be important, ie $f\big(g(x)\big) = g$. Such functions exist, but mostly are two-way, ie finding inverse functions is easy work eg. such a function is $f(x) = 2x$
A practical example of these functions is the electrical switch. However, these functions are not usable in cryptography. The most important are the concrete forms of so-called one-way functions. These functions appear to find their inverse functions, which are found through complex procedures. So for a given x we can easily compute $f(x)$, but for given $f(x)$ it is difficult to measure x, but if the secret value is known, then, both the direct value and the inverse value are easily counted. Modular arithmetic means the presence of a large number of such one-time functions. So in this section we will explore to find such functions.

Keywords: One-way, inverse, encryption, DH protocol.

Composite functions

Let be given the function $f\colon X \to Y$ and the function $g\colon T \to Z$ (see Fig.1).
DEFINITION 1.1. THE COMPOSITE FUNCTION OF THE INTERNAL FUNCTION f AND OF THE EXTERNAL FUNCTION g IS CALLED THE FUNCTION OF X TO Z SUCH THAT IN EACH ELEMENT $x \in X$, WHERE IS DEFINED, HAS THE VALUE $g\ (f\ (x))$. [7]

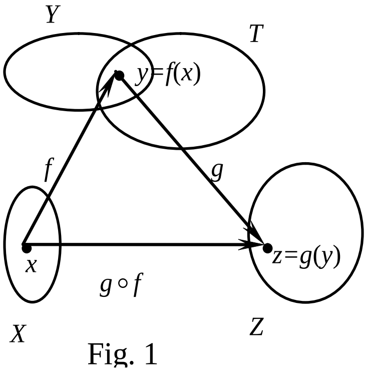

Fig. 1

Such function is marked $g \circ f$ (reads "g circle f"). From the definition we have $(g \circ f)\,(x) = g\,(f(x))$ for each $x \in D\,(g \circ f)$. In particular case when f and g are such reflections that $f\colon X \to Y$ and $g\colon Y \to Z$, it is shown that $g \circ f$ is a reflection of X in Z, which is called a composite reflection. So in this case for every $x \in X$ we have $(g \circ f)\,(x) = g\,(f\,(x))$.
Example 1.1. Let be given the functions $f\colon x \mapsto 2^x, x \in R$ and $g\colon x \mapsto 2x, x \in R$. To be found $(g \circ f)\,(x)$ and $(f \circ g)\,(x)$.
The examples of functions f, g are respectively $f(x) = 2^x$ and $g(x) = 2x$. Therefore from the above we have:

$(g \circ f\,)(x) = g(f(x)) = g(2^x) = 2 \cdot 2^x = 2^{x+1}$;

$(f \circ g)(x) = f(g(x)) = f(2x) = 2^{2x}$.

By the way of example, we observe that in general the commu- nity role does not apply to composite functions. So, $f \circ g \neq g \circ f$.
Cases, where relevant $f \circ g = g \circ f$., are called composite commodity functions. In particular, this property enjoys the bureaucratic functions with their inverses. Thus $f\left(f^{-1}(x)\right) = f^{-1}\left(f(x)\right) = x$

Cryptography and basic concepts

By cryptography or cryptographic system (also cryptosystem, code) we mean the transformation of an open text message by means of a ciphering function (or simply encryption) in such way that only an authorized receiver can return the message transformed into the first state. The process of transforming open text into encrypted text (or cryptogram) is called a cipher and if any encryption function is determined by a ciphering algorithm that is common to each encryption function of a given family and a key k, which is parameter of a special transformation. [3] [4] [5].

Definition 2.1: The cryptosystem is called 5-tupled (P, C, K, E, D) that satisfies the conditions:

- P, is a finite family of all open texts.
- C, is a finite family of all encrypted texts.
- K, the key space, is a finite family of all possible keys.
- The elements E and D are reflections of P in C and C in P such that for each $k \in K$ there is a cipher rule $e_k \in E$ and a decoding rule $d_k \in D$ that $\forall x \in P$, $d_k\left(e_k(x)\right) = x$.

An important case of classical forms of cryptosystems is when the sender and receiver use the same key k (in this same sense the keys are also considered when the recognition of one which automatically introduces the other). These systems are called single key cryptosystems to distinguish them from cryptosystems using two different keys, called public key systems. Such systems are quite suitable for protecting information transmitted over a computer network, or to encrypt personal user files. [2]

The cryptographic systems are classified into two types:

1. Secret key cryptography
2. Public key cryptography

Secret key cryptography is the oldest type of secret mark. There are two main types of cryptography with a secret key:

1. With displacement
2. With replacement

The shift digit encrypts the original message by changing the order of the characters where they appear. Instead, the original message is encrypted by replacing some characters with some other characters. In both types both the sender and the receiver distribute the same secret key.

Public key cryptography uses two keys, a public key known to everyone, and a private key or secret known only to the recipient of the message.

Public key cryptography is important that the public key and secret are linked in such a way that only the public key can be used to encrypt messages and only the secret key can be used for their decryption.

Asymmetric cryptography uses two keys that are related to each other with mathematical relationships. One of them is private and used to encrypt the document while the other is public and used only to decrypt the document.

In cryptography the key is a variable value that is applied using an algorithm to a block or string of unscripted or encrypted text. The length of the key is a factor when it is considered how difficult it is to decrypt the text in the message. In the concept of the database, the key is a field selected for sorting. The primary key is the unique key to any data and as such is used to access that given. The external key, is the key that shows the primary key on another table.

In cryptography, a private key or secret is a key encryption / decryption known only by the parties that exchange the message. In the traditional cryptography of the secret keys, a key will be distributed between the communicators so that each of them can encrypt and decrypt messages.

The risk of this system is that if any person loses the key, or the key is stolen by someone, the whole system fails. A recent alternative is the combination of private and public keys. In this system, the public key is used with the secret key.

In cryptography, the public key is a value given by a certain authority, as a key encryption which together with the private key, taken from the public key, can be used to encrypt digital messages and signatures. The combined use of public and private keys is known as asymmetric cryptography. The system using Public key is called the Public Key Infrastructure (PKI). [11]

Diffie-Hellman Protocols

The main problem with these functions is that it is not proven the strict mathematical existence of both functions and trapping functions. In addition, there are two functions that are considered candidates with the above mentioned features:

- Discrete exponential function is the inverse function of the discrete logarithmic function
- Producing full numbers that is the inverse function of factoring the number obtained

The functions mentioned are easily counted, while it is believed that this is not the case with their inverse functions.

The abbreviation "DH" will be used for the algorithm Difi-Hellman or the switching protocol of the keys. The protocol is developed independently in two places and represents an algorithm for changing common symmetric keys. No encryption or digital signature is envisaged. The security of the DH algorithm is based on the difficult calculations of functions in the disrcete logarithm for the values given g, p and $g^n mod\ p$ to be found n?

For the known values g and x, where $x = g^n$, it can be computed at, as $n = \log_g x$

If $x = g^n\ mod\ p$, also n can be matched by logs but through a disrcete logarithm.

Below we will take the math base of DH algorithms [6]:

Step 0. Let p be a prime large number and g such that for any one $x \in \{1, 2, 3, \ldots, p-1\}$ can be matched by n, through $x = g^n\ mod\ p$. The p and g values are public. In communication, for example, between Albina and Altin, these parameters can determine which of these two and then these are exchanged through the public channel. Albina selects its secret value a, Altin selects its secret value b. These values should be prime large numbers.

Step 1. Albina publicly sends Altin the value $g^a\ mod\ p$. While Altin publicly sends Albina $g^b\ mod\ p$.

Step 2. Both on the basis of accepted values measure the common secret value $g^{ab}\ mod\ p$. The gained secret value can be used as a symmetric key.

Step 3. Albina and Altini use the value $g^{ab}\ mod\ p$ as a symmetric key.

A third person can disclose the values $g^a\ mod\ p$ and $g^b\ mod\ p$, as they are exchanged through the public channel. However, the third person can not detect a and b values, if this happens, so the system is broken and this means that the problem of disrcete logarithm is solved [6].

In standard PKSC # 3 Diffie-Hellman Key Agreement Standard, the parameters values a, b, g and p are predefined and preferred to generate and to exchange the common symmetric key. In practice for p is used a very large number that is larger than 1024 bits**.**

Example 3.1.

We select public parameters p and g

$p = 33, \quad g = 3$

Select secret parameters a and b

$a = 11$ and $b = 7$

Albina sends the value $A_a = g^a\ mod\ p = 3^{11}\ mod 33 = 3$.

Altin sends the value $A_b = g^b\ mod\ p = 3^7\ mod 33 = 9$.

Albina recognizes the key $K_{Albina} = {A_b}^a\ mod\ p = (g^b\ mod\ p)^a\ mod\ p = 9^{11}\ mod 33 = 9 \Rightarrow$

$$K_{Albina} = g^{ab}\ mod\ p = 3^{77}\ mod 33 = 9.$$

Altin recognizes the key $K_{Altin} = {A_a}^b\ mod\ p = (g^a\ mod\ p)^b\ mod\ p = 3^7\ mod 33 = 9 \Rightarrow$

$$K_{Altin} = g^{ab}\ mod\ p = 3^{77}\ mod 33 = 9.$$

Well, $K_{Albina} = K_{Altin} = 9$.

In the example, we used prime small numbers in order to make the simplest sense of DH protocol, but in practice we work with simple large numbers.

As mentioned above a third person can enter the communication, so for safer communication, authentication mechanisms must be provided, which means that the two people who are in communication must be safe in the integrity of the exchange of messages. We must always be aware of the existence of such attacks in communication.

Conclusion: After setting the symmetric key as above, the encoder and decoders in further works have some kind of cryptosystems that use the symmetric key.

References

1. Bruce Schneier .”Applied Cryptography” , 1996
2. I. Damgard. Towards practical public key cryptosystems secure againstchosen ciphertext attacks. In Advances in Cryptology.
3. D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. In23rd Annual ACM Symposium on Theory of Computing,1991.
4. D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography, 1998.
5. C. Dwork and M. Naor. Method for message authentication from non-malleable cryptosystems, 1996.
6. M. Veinovic, S. Adamovic, Kriptologija 1, 2013
7. K. Filipi, A. Jusufi, Xh. Beqiri, Matematika për ekonomistë, Tetovë, 2012