CS 333 Project Report

Egemen İşcan
egemen.iscan@ozu.edu.tr

Hasan Erdem Bilgin
hasan.bilgin@ozu.edu.tr

Yamaç Demirkan Yılmaz
demirkan.yilmaz@ozu.edu.tr

Peker Çelik
peker.celik@ozu.edu.tr

June 2021

Contents

I. Introduction

In this article, we will discuss a new way of transmitting and receiving any kind of information in an electronic environment with a simple but very secure encryption method. It is very crucial to preserve the validity of a message when transmitting it to its correspondent. Paper messages have two important qualifications. The first one is that they are private, covered in an envelope and they are sealed, so nobody except the correspondent cannot read them. The second is that they are signed by an authority, therefore the correspondent would know that this message is actually coming from the intended sender. All our effort is to protect these properties of a message while transmitting and receiving them in an electronic system by developing a new encryption method.

To ensure these two crucial properties of a message, we have come up with a public key cryptography implementation, which was originally proposed by Diffie and Hellman. Public key cryptography means that each user, for instance, the sender and the receiver, stores a unique encryption method in a publicly visible file. Again, each user would have to come up with a unique decryption method to decrypt the messages, but this time, they will store their decryption methods in a secret place.

Different from Diffie and Hellman's proposal, we are going to present an implementation of the system in action in the upcoming sections.

II. Background

In this section, we will briefly describe the Public-Key Cryptosystems and the advantages that provide us like privacy and signature.

A. Public-Key Cryptosystems

Public-Key Cryptosystems have two main procedures. Those are encryption (E) and decryption (D). Encryption procedure (E) is published publicly for each user. However, the decryption procedure (D) must be kept private. These procedures have the following four properties:

a. Deciphering an encrypted message (M') results in getting the original message. In math notation:

$$D(E(M)) = M \tag{1}$$
$$D(M') = M$$

b. Both E and D are computed easily.

c. Revealing E publicly does not cause any vulnerability because revealing E does not get computed D easier. This means that only the receiver who has D can see the messages encrypted with E.

d. Because of the mathematical concept of Public-Key Cryptosystems also, E and D is reverse, following notation is also correct.

$$E(D(M)) = M \tag{2}$$

Procedures have a general method and a secret key. The method encrypts the message (M) to the form called ciphertext (C). Everybody can use the same method unless the key is revealed. If so, vulnerability occurs. Presenting E does not provide any practical approach to find out D based on the workload of the computation.

Any function that satisfies (a) - (c) is known as the ”trap-door one-way function”. Trap-door functions are the functions that cannot be reversed. Therefore the only way of revealing the function is brute force, which is impractical. The property (d) is necessary for signing the message. In the next chapters, we will show some scenarios that we suppose Alice (A) and Bob (B) use this cryptosystem to communicate and they use E_A, D_A, E_B, D_B.

B. Signatures

A signature is a stamp on a message that uniquely identifies the sender. As we mentioned in the previous section, Bob sends Alice a message. The requirements that we need to satisfy are that the message needs to be encrypted, only Alice must be able to decrypt the message and Alice must be sure that the sender is Bob. So let's see how it is done.

Bob encrypts the message M with his Decrypt function D_B and creates signature S. Then Bob encrypts his signature S with the encrypt function of Alice E_A to get M. Then Alice receives the encrypted message. First Alice uses E_B to get the signature after that uses his private D_A to get the message. Since if the sender was not Bob E_B would not get us the signature. In mathematical terms:

$$S = D_B(M)$$

$$E_B(S) = E_B(D_B(M)) = M$$

Bob computes $E_A(D_B(M))$ to get the encrypted version of the signature, which includes the message at the same time. And all Alice need to do is decrypt the message with Her decrypt method D_A and use the public method of Bob E_B to transform the signature to a readable message.

C. Privacy

Encryption is the standard means of rendering a communication private. Let's call Charlie and listen to the conversation between Alice and Bob. The aim of this system is to make Charlie read garbage, in other words, encrypted messages which actually include the context and signature at the same time. Unless any private key or Decrypt method is leaked, the encryption is quite unbreakable based on the computation necessary and one-way trap function that we use due to Diffie and Hellman. Using two encryption that Bobs signature and Alice's Encryption function consists of the sender Bobs identified correctly and only Alice can read the message. Also changing the keys and using different keys per conversation increases the level of privacy.

III. Our Encryption and Decryption Methods

We assign the letter M for the message to be encrypted, and the pair of integers (e, n) signifies the public key, where $e \geq 0$, $n \geq 0$. If message M is larger than n, it is required to break into smaller parts where each message is between 0 and n-1. The encryption and decryption algorithms may then be computed as follows:

Raising M to the power e modulo n:

$$C \equiv E(M) \equiv M^e$$

Then you may raise C from the previous part to power d modulo n, in order to compute the decryption algorithm D:

$$D(C) \equiv C^d$$

Keep in mind that an encrypted message is not larger than the original. The encryption key is the pair of (e, n) and the decryption key is the pair of (d, n). For each user, the encryption key is left public while the corresponding decryption key is kept private.

In order to choose the encryption and decryption keys, we should determine two very large prime numbers and assign their product to the public variable n.

$$n = p \cdot q$$

Since the primes p and q are large, this will make them difficult to reveal because factoring n is computationally impractical. This also obscures the method of deducing d from e.

Then pick an integer d, preferably a large random integer, which satisfies the following condition:

$$gcd(d,\ (p-1)\cdot(q-1)) = 1 \qquad (gcd\ standing\ for\ ''greatest\ common\ divisor'')$$

The reciprocal for d modulo (p-1).(q-1) is the integer e which is derived from p, q and d:

$$e \cdot d \equiv 1\ (mod\ (p-1)\cdot(q-1)) \tag{3}$$

IV. The Underlying Mathematics

Fermat-Euler theorem (or Euler's totient theorem) states that $a^{\phi(n)} \equiv 1\ (mod\ n)$ if a is coprime to the modulus n, where ϕ is Euler's totient function. The output of this function is the number of integers greater than 0 that are relatively prime to n.

We use this theorem to show that the deciphering algorithm is correct by plugging M in place of a where M is relatively prime to n,

$$M^{\phi(n)} \equiv 1\ (mod\ n) \tag{4}$$

Therefore, for prime numbers p,

$$\phi(p) = p - 1$$

If n = p · q, by a fundamental property of the totient function we have

$$\phi(n) = \phi(p) \cdot \phi(q)$$

Using both of the properties above

$$\begin{aligned}\phi(n) &= (p-1)\cdot(q-1)\\ &= n-(p+q)+1 \qquad (5)\end{aligned}$$

As we have already demonstrated (3) d·e is relatively prime to (p-1) · (q-1) which were also shown to be equal to ϕ(n).

$$e \cdot d \equiv 1 \ (mod\ \phi(n))$$

We can now prove that (1) and (2) hold

$$D(E(M)) \equiv (E(M))^d \equiv (M^e)^d \ (mod\ n) = M^{e\cdot d} \ (mod\ n)$$

$$E(D(M)) \equiv (D(M))^e \equiv (M^d)^e \ (mod\ n) = M^{e\cdot d} \ (mod\ n)$$

And so

$$M^{e\cdot d} \equiv M^{k\cdot\phi(n)+1} \ (mod\ n)$$

Observe the two following equations

$$M^{\phi(n)} \equiv 1 \ (mod\ n)$$

$$M^{p-1} \equiv 1 \ (mod\ p)$$

From which we derive the below equation since we have shown in (5) that (p-1) divides ϕ(n).

$$M^{k\cdot\phi(n)+1} \equiv M \ (mod\ p)$$

When $M \equiv 0\ (mod\ p)$ is true, it implies that the above statement is also true. Therefore this equality is valid for all M. When we apply the same reasoning to q, we get

$$M^{k\cdot\phi(n)+1} \equiv M\ (mod\ q)$$

Here, the last two equations combined mean that for all M

$$M^{e\cdot d} \equiv M^{k\cdot\phi(n)+1} \equiv M\ (mod\ n)$$

We can draw the conclusion that consequently, (1) and (2) hold for all M where $0 \leq M < n$. Hence, D and E are an example of reciprocal permutations.