An Exploration of Modern Cryptography

Siddharth
Mahendraker

March 18, 2012

Abstract

Fusce dapibus, tellus ac cursus commodo, tortor mauris condimentum nibh, ut fermentum massa justo sit amet risus. Maecenas sed diam eget risus varius blandit sit amet non magna. Duis mollis, est non commodo luctus, nisi erat porttitor ligula, eget lacinia odio sem nec elit. Vivamus sagittis lacus vel augue laoreet rutrum faucibus dolor auctor. Aenean eu leo quam. Pellentesque ornare sem lacinia quam venenatis vestibulum. Nulla vitae elit libero, a pharetra augue. Donec id elit non mi porta gravida at eget metus.

Contents

Introduction

Suppose two people, Alice and Bob, wish to communicate by mail and do not want their mailwoman, Eve, to be able to read their messages. Alice and Bob are military personal of the same country, but they have never met each other before. Because Eve is the mailwoman, she will be able to read all of the messages passing between Alice and Bob, but her obligation to the postal service prevents her from tampering with these messages[1].

The question is, is it possible for Alice and Bob to communicate securly in these circumstances? Astoundingly, the answer is yes!

Cryptography is the science of securly sending messages over insecure channels. Using cryptographic techniques, Alice and Bob can be sure that their communications are illegible to Eve.

0.1 Terminology and Basic Concepts

0.1.1 Alice and Bob

Unless specified otherwise, Alice and Bob are two parties attempting to communicate over an insecure channel, and Eve is their adversary trying to read their messages.

0.1.2 Encryption and Decryption

Messages in cryptography are formally called plaintext. When messages are scrambled, or made "illegible", they are encrypted. The encrypted form of these messages is called ciphertext. The reverse process of encryption, decryption, accepts ciphertext as input and returns plaintext. We can describe this mathematically as:

$$E(M) = C$$
$$E'(C) = D(C) = M$$

Where M denotes plaintext, C denotes cipher text, E is the encryption function and D is the decryption function, or the inverse of E. Also note

[1] In reality, Eve would not be bound by such a petty obligation, however, for the sake of simplicity, let us assume this is true.

the following identity:

$$D(E(M)) = M$$
$$E(D(C)) = C$$

0.1.3 Ciphers and Keys

A cryptographic algorithm, or cipher, is a function used for encryption and decryption.

If the workings of a cipher are made public, then the messages of anyone who is known to use the cipher can quickly be comprimised by simply implementing an inverse of the cipher. Therefore, cryptographers introduced a key. A key is a piece of secret, private information upon which the cipher depends. It often takes the form of a number. The total number of possible values a key can take on is called they keyspace. Because ciphers depend on the key to encrypt and decrypt plaintext, encryption and decryption is often denoted:

$$E_K(P) = C$$
$$D_K(C) = P$$

The key is denoted by K and the keyspace is by $\mathcal{K}$. Note that the identity mentioned in 0.1.2 still holds true for ciphers.

0.1.4 Symmetric and Asymmetric Ciphers

There are two distict kinds of ciphers, symmetric ciphers and public-key (or asymmetric) ciphers.

Symmetric ciphers are ciphers for which the key used to decrypt ciphertext and encrypt plaintext is the same. In most symmetric ciphers, this means that Alice and Bob will need to agree on a key before they can begin sending messages. Symmetric ciphers can be further categorized as stream ciphers or block ciphers. Stream ciphers operate on only one bit (or byte) of plaintext at a time, where as block ciphers operate on a large number of bytes at once.

Public-key ciphers are ciphers for which the the key used for encrypting plaintext is different from the the key used for decrypting ciphertext. Further, these keys should be independant of each other, meaning the decryption key can not be calculated[2]from the encryption key. The design of this

cipher is such that the ecryption key can be published for anyone to use, but only the owner of the decryption key can decrypt the message. This is why is encryption key is referred to as the public key and the decryption key is referred to as the private key.

1 Substitution Ciphers

A substitution cipher is a cipher which

The first cipher we will be analyzing is a substitution cipher called the Caesar cipher. In ancient times the Caesar cipher was used by Caesar and his generals to pass along messages on the battle field. Originally, the cipher shifted it's input 3 characters to the right. Therefore, text such as:

```
the quick brown fox jumped over the lazy dog
```

becomes

```
wkh txlfn eurzq ira mxpsv ryhu wkh odcb grj.
```

Although this looks complex, the flaws in this cipher will soon be all too aparent.

2 Block Ciphers

3 ECC - Elliptic Curve Cryptography

[2]In a reasonably amount of time ofcourse.