University Of Agder

DAT 211

Networking and Security

Cryptographic concepts

Author:
Bendik Egenes Dyrli

Supervisor:
Sigurd Kristian Brinch

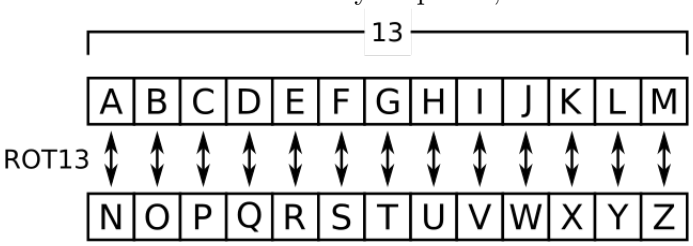
2015

Introduction

cryptography is a practice or you could call it an art so to speak, this art is over 4000 years old and predates computers or any technology. Cryptography is the practice of both hiding and revealing information. It's been widely used in all of the computers and software to this day ,and encrypting data is starting to be a trend, people want to secure their data so that unwanted people can't see what they are doing both online and offline. In this essay we'll take a look at a few of the different concepts there is in cryptography, and find out how secure they are and if they could or should be used.

Caesar cipher - Shift Chipher

The Caesar chiper is what you call a shift chiper, it fucntions by changing the character for another one. It works in the manner that you take the first letter of the word you want to encrypt like for example the word is **DAT211**, then you take the 'D' and you shift it by 13 places so the 'D' is now a 'Q' and you do this until the whole word is encrypted, thou this can only be done with the letters, so the number will be as it is. so the finished word, encrypted with rot13 will be **QNG211**. The word rot is short for rotation, since before they used to have these disc's where they'll input the first encrypted letter then rotate the disc by 13 places, and it would return the first decrypted letter.[1]



Vigenere Table

Vigenere Table is a multi-alphabet substitution. You have a 26x26 table with letters from **A - Z**.So how it works is that you have a message you want to decrypt, so you'll go to the first letter on the alphabet that is the first letter of your message and then find a letter on the the other alphabet. Example we have a Message:**DAT211**, and the keyword:**ROT211** with this we'll get the encrypted message:**UOM211**. To decrypt this message you'll need the encrypted message and the keyword, if you only have the encrypted message and not the keyword or vice versa there is no way that you'll be able to decrypt the message. [2]

Asymmetric cryptography (public-key cryptography)

Asymmetric key is the kind of way that most people use when they would like to encrypt a message. They encrypt a message, sends it to a person and then give that person a public key which then will make that person able to read the message. Example; ssh(secure shell) to ensure that the communication between the client and the host. Instead of using a password, you could use an asymmetric key where you generate a public key which is placed on the server and a private key that you'll use when connecting to the server. [3]

Conclusion

Now in this essay we've seen that you can encrypt your information with concepts like rot13 and Vigenere Table. These ways are pretty simple to decrypt so to speak, but if you wanted a more secure way of encrypting information you could use something like an Asymmetric key. This way you can encrypt a message with a private key, and then send the public key around to other people who's going to read the hidden message. Asymetric key or Public-Key cryptography is how most people encrypt their messages.

References

[1] "Caesar's Method – from Wolfram MathWorld", Mathworld.wolfram.com. [Online]
http://mathworld.wolfram.com/CaesarsMethod.html
[Accessed: 20- Mar- 2016]

[2] "The Vigenre Cipher Encryption and Decryption", Cs.mtu.edu. [Online]
http://www.cs.mtu.edu/ shene/NSF-4/Tutorial/VIG/Vig-Base.html
[Accessed: 20- Mar- 2016]

[3] What is asymmetric cryptography (public-key cryptography)? SearchSecurity [Online]
http://searchsecurity.techtarget.com/definition/asymmetric-cryptography
[Accessed: 20- Mar- 2016]