A Study on Network Security Services with Cryptography and an Implementation of Vigenere-Multiplicative Cipher

Khandoker Abdul Rahad
Institute of Information Technology
Jahangirnagar University
Savar, Dhaka
Rahad.baten@yahoo.com

Sayed Mohsin Reza
Institute of Information Technology
Jahangirnagar University
Savar, Dhaka
smrezaiit@gmail.com

Abstract- Different types of encryption techniques are used for many years to secure the information. The purpose of this paper is to construct a new method named as Vigenere-Multiplicative cipher. Here we develop the algorithm and its algebraic description. In addition, we provide the frequency analysis of this method. Further, implementation of the method, security attacks, comparisons between given cipher and most common ciphers are briefly discussed.

Keywords: Network Security, Encryption, Vigenere Cipher, Multiplicative Cipher, Encryption Standards etc.

I. Introduction

Development in communication has brought unknown people together through information technology. We are all familiar with the internet, however, web applications out of these that most of us uses are unsafe browsing facilities. There are lots of transactions happening everyday .We have to make sure that these transactions are safe and secure. This technology is known to us as encryption. The internet has so many connections, as we do not have control over the activities such as hacking, sniffing, breach of conduct, and etc. For this we have to come up with a system that is totally impossible to break.

Cryptography is a tool that can be used to keep information confidential and to ensure its integrity and authenticity. All modern cryptographic system are based on Kirchhoff's principle of having a publicly-known algorithm and a secret key. Many cryptographic algorithms use complex transformation involving sub-situations and permutations to transform the plaintext into cipher text. Cryptographic algorithm can be divided into symmetric –key algorithms and public-key algorithms. [1]

II. Art of Communication

In Network Security, Art of communication provides two types of action: Encryption and Decryption. To secure data transfer we have to encrypt our data by scrambling our information. After scrambling the information, it is quite impossible to understand by a third party.

To retrieve the encrypted information properly, we have to decrypt the scrambling information. It enables the receiver to get the exact information. [2]

Even if we really understand what how encryption plays a part in our day-to-day life, but we use it often. As most of the businesses completely depended upon the internet for buying, selling, and transferring money over e-banking system, organizing, teleconferencing, and providing various other services these all need encryption for safe connection and privacy. [3]

Computers in the early form of development did not have networking facility. As the growth of computer networking industry, there are more software that more readily available for individuals. The advantage of the doing business over the internet is performed and, thus, to keep the unauthorized people away from hacking, network encryption has been started.

III. Model of Network Security

Model of computer network security has some basic structure as follows [3]

1) Network Security and their scenario must be included in the algorithm.
2) A proper mathematical function should be developed in the algorithm.
3) Business relevant property with authentication must be declared.
4) Shared key, Protocol of the method should be defined.

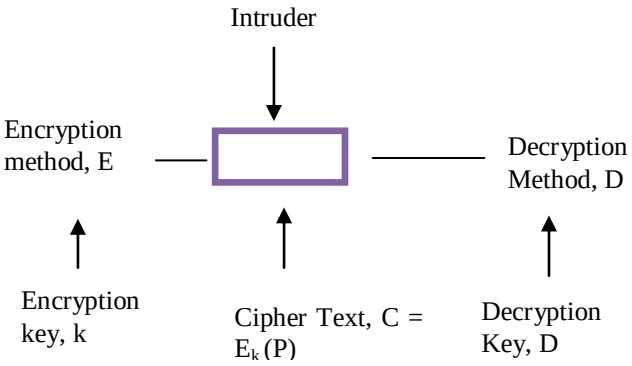

Fig. 1: The encryption model

A mathematical function of the encryption technique with shared key enables the sender to scrambles the message. The output of encryption process is then transmitted, often by a program or software. We assume that the hacker or intruder receives the complete cipher text. However, unlike the intended recipient of the information, the hacker does not know what the decryption key is and so can not decrypt the cipher text easily.[1]

IV. Classification of Encryption

Cryptography algorithms can be divided into two groups symmetric-key cryptography algorithms and asymmetric cryptography algorithms. [4]

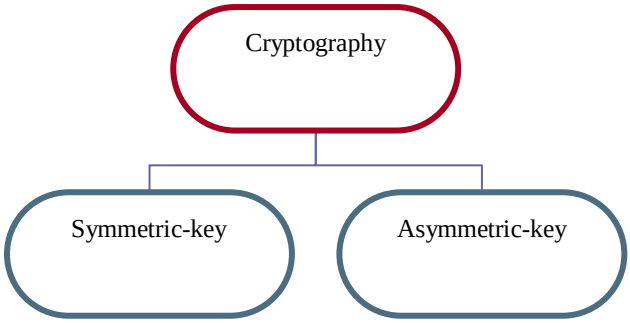

Fig. 2: categories of cryptography

A. *Symmetric-key*

Symmetric-key cryptography is the same key that is used by both encryption and decryption. It is also called single key encryption.

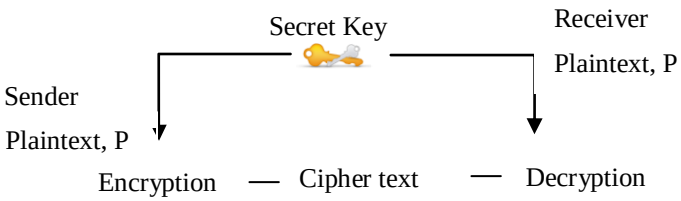

Fig. 3: Symmetric key

Symmetric key Algorithm types:

Stream cipher: plaintext are encrypted one at a time. This conversion varying digits.

For instance,

Plaintext, P = “LAPTOP”
Cipher Text, C = “MBQUPQ”
Block Cipher: plaintext with block are encrypted. Length and unvarying digits has been fixed for each block.

For instance,

Plaintext, P = “LAPTOP”
Cipher Text, C = “13 11 53 44 43 53”

B. *Asymmetric-key*

Asymmetric-key uses two different keys for encryption and decryption. One is public key and another is private key. Public key is used for the encryption and private key is used for decryption. Symmetric key encryption does not provide as much security. Hence, the importance of the asymmetric key, also known as public key encryption, is greater.

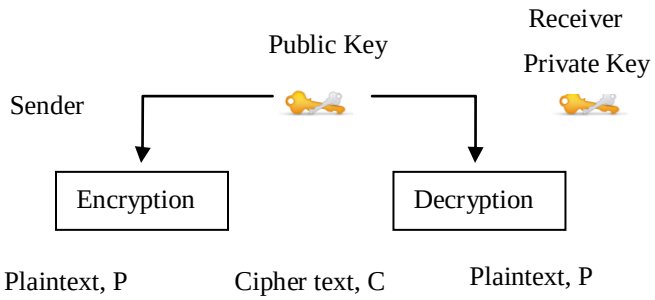

Fig. 4: Asymmetric Key

Asymmetric key has the combination of public key and private key. private key is used by internal host. At the mean time the public key is given to other computers with which it is able to communicate securely.[3]

1)RSA

The most common public key algorithm is RSA. The RSA stands for the last names of the inventors Ron Rivest, Adi Shamir, and Leonard Adleman. They developed this algorithm in 1978. Since then it is widely used. It uses two numbers e and d, as the public and private keys. There is a special relationship between e and d. [4]

RSA provides more data security that's why other algorithms does not cope the RSA. Mathematically, RSA is so strong to maintain the privacy of the message.

2) Public Key Infrastructure (PKI)

For data security in network, we have to develop the keys by using which the information should be transferred. For these purposes, a well known organization distribute, maintain the rules named as Public-key infrastructure (PKI). It relies on a set of unique keys with a mathematical function. Each pair of keys has a public key and a private key. The public key, which is published to users within the public domain, the private key is private for each entity. With public key Infrastructure (PKI) the encrypted data is transmitted to the public key of the recipient. To unlock the encrypted data or information, we use private key as like as a digital signatures. [8]

3) Certificate Authority (CA)

An entity that issues digital certificate named as Certificate authority (CA). This helps relying parties to rely upon signatures made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the owner of the certificate and the party or user relying upon the certificate. CA's are characteristic of many public key infrastructure (PKI) schemes. Certificate authority only can issue the Digital Certificate, which contains both the public and private key for encryption and decryption of the information. Depending upon the volume of the identity verification, Certificate Authority can issue Digital Certificate for different level of trust. [9]

4) Registration Authorities (RAs)

Registration Authorities(RAs) have similar functionality as like as CA. The RA can issue the temporary digital certificates. The validation of temporary digital certificates are limited. And it is not fully trustable, unless CA verifies them. A Registration Authority (RA) is a subsystem that accepts enrollment requests and authenticates them in a local context .Upon successful authentication, the RA then forwards the enrollment request to the designated Certificate Authority (CA) to generate the certificate. Based upon the type of enrollment, they can develop appropriate plugins to authenticate the request. [9]

5) Digital Certificates for authentication

Digital certificates are used to authenticate the identity of a computer or a company through Certificate Authority (CA). It can also be used to retrieve rights and authority. Most commonly, it is rapidly used in Ecommerce. To build up the trust between Customer and the authority, Digital certificate plays a vital role. Ecommerce sites have public digital certificates that anybody can view to build up the trust. [3]

V. CIPHER: ALGORITHM IN CRYPTOGRAPHY

Every Sender-Receiver pair needs their very own unique cipher for a secure communication. Millions of communication pairs can be served by one cipher. Now, question is how the cipher is created? We want to secure the communication by creating the cipher as complex as it is unique. Blaise De Vigenere, a French Mathematician tried to create a secret key stream. In a Vigenere Cipher, each letter is shifted in sequence with different shift values. This cipher consists of Caesar ciphers. [1]

Let,

Plaintext, $P = P_1P_2P_3...$
Key Stream, $K = [(K_1K_2K_3...), (K_1K_2K_3...)...]$
Encrypted Text, $C_i = (P_i + K_i) \bmod 26$
Cipher Text, $C = C_1C_2C_3...$

On the other hand, Multiplicative cipher works as the key multiple with plaintext. At the decryption time, we find the message calculating the multiple inverses with Cipher Text.

Let,

Plaintext = P
Key = k_m
Cipher Text, $C= (P * K_m) \bmod 26$

Now, we implement these two ciphers to evaluate a new combination. It works as powerful algorithm with more security and more unique. [4]

VI. Idea of Vigenere-Multiplicative Cipher

The multiplicative cipher is substituting the letter so that it should not be exposed. And the Vigenere cipher is simple enough to be a field cipher if it is used in conjunction with cipher disks. Combination of these two resources can make a more secure cipher.

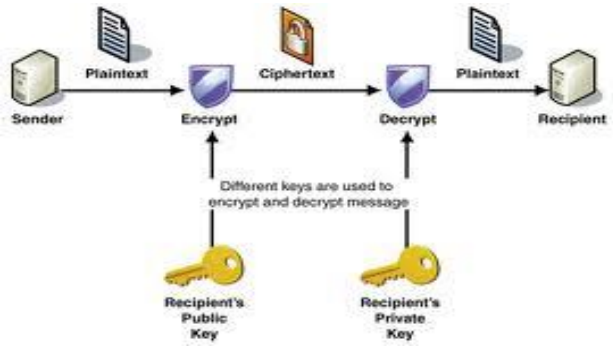

Fig. 5: The Vigenere-Multiplicative Cipher

A. Scenario:

1. Encryption Process

The Vigenere Cipher creates the ciphers by concatenating the encrypted text, and then modifying that text to Cipher Text. In the Vigenere-Multiplicative cipher, we think about those cipher text as Half Cipher Text.

This Half Cipher Text is used as next plaintext of Multiplicative Cipher Text. We assume that, after multiplicative cipher, the original cipher text is introduced.

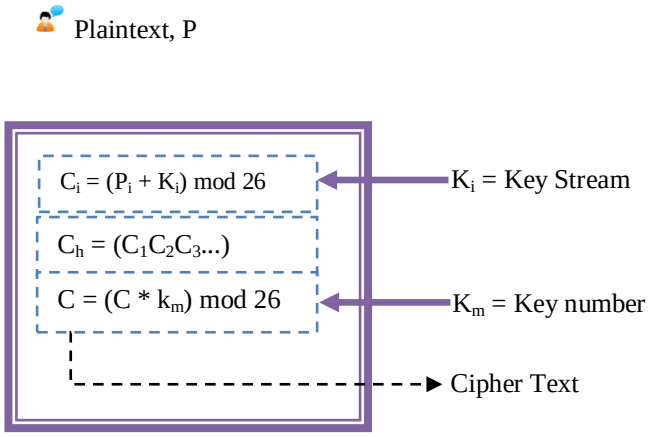

Fig. 6: Eencryption Scenario

2. Decryption Process

We have to figure out the decryption process of the proposed Vigenere-multiplicative cipher. After encryption, we have encrypted/ cipher text.

At first, we have to find out the multiplicative inverse of key number. Then, cipher text multiply with the multiplicative inverse number of the key. It produces the half plaintext as our algorithm.

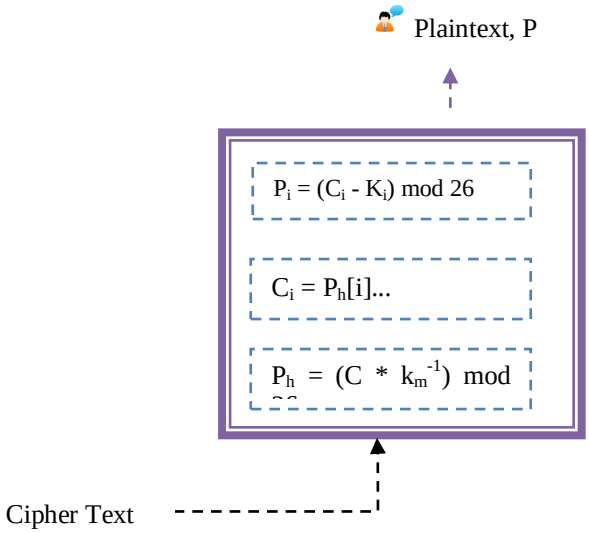

Fig. 7: decryption Scenario

B. Algebraic Description:

Vigenere-Multiplicative can also be viewed algebraically. If the letters A–Z are taken to be the numbers 0–25, and addition is performed modulus of 26, then Vigenere-Multiplicative encryption E using the key K can be written,

Encrypted Text, $C_i = E_k(M_i) = (P_i + K_i) \bmod 26$
Half Cipher Text, $C_h = C_1C_2C_3...$
Full Cipher Text, $C = (C_h * k) \bmod 26$
And decryption D using the key K_i and K_m.
Half Plain Text, $P_h = D_{km}(C) = (C * k_m^{-1}) \bmod 26$
Cipher Text, $C_i = P_h[i]$
Plain Text $P_i = (C_i - K_i) \bmod 26$

C. Example of Vigenere- Multiplicative Cipher

Encrypt the message “I am studying.” using Vigenere cipher with the 6-character keyword “mobile” and a key of $K_m = 7$ using multiplicative cipher.

Solution:

Step 1: Key Stream: ‘MOBILE’

Letter	Value
M	12
O	14
B	01
I	08
L	11
E	04

Step 2: Using Formula: $C_i = (P_i + K_i) \bmod 26$

Plain Text	P's values	Key Stream	HC's values	half Cipher Text
i	08	12	20	U
a	00	14	14	O
m	12	01	13	N
s	18	08	00	A
t	19	11	04	E
u	20	04	24	Y
d	03	12	15	P
y	24	14	12	M
i	08	01	09	J
n	13	08	21	V
g	06	11	17	R

Half Cipher text is " UONAEYPMJVR"

Step 3: Using Formula: $C = (C_h * K_m) \bmod 26$

half Cipher Text	HC's values	cipher text	Cipher text
U	20	10	K
O	14	20	U
N	13	13	N
A	00	00	A
E	04	02	C
Y	24	12	M
P	15	01	B
M	12	06	G
J	09	11	L
V	21	17	R
R	17	15	P

The original Cipher Text: "KUNACMBGLRP"

Step 4: using the formula $P_h = (C * K_m^{-1}) \bmod 26$.

Cipher text	C's values	P_h's values	Key Stream	P's values	Plain Text
K	10	20	12	08	I
U	20	14	14	00	A
N	13	13	01	12	M
A	00	00	08	18	S
C	02	04	11	19	T
M	12	24	04	20	U
B	01	15	12	03	D
G	06	12	14	24	Y
L	11	09	01	08	I
R	17	21	08	13	N
P	15	17	11	06	G

Here, $K_m = 7$ so $K_m^{-1} = 15$. Then use the plaintext value $P = (P_h - K_i) \bmod 26$.

The message is "I am studying".

D. Frequency Analysis

In the Vigenere-Multiplicative Cipher, there is less percentage to discover shifted plaintext frequencies. But in Vigenere Cipher, once every letter in the key is known, the cryptanalyst can simply decrypt the cipher text and reveal the plaintext.

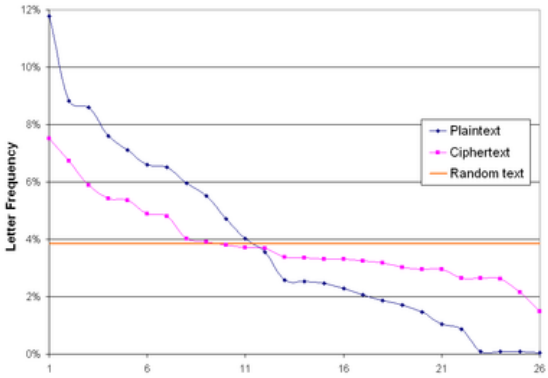

Fig. 8: Letter Frequency in Vigenere Cipher

For Example, if P is the most frequent letter in a cipher text whose plaintext is in English, one might suspect that P corresponds to E, because E is the most frequently used letter in English. But in our Vigenere-Multiplicative Cipher, There is random Number of cipher Text of Letter P.

Another weakness of the Vigenere cipher is the repeating nature of its key. If a cryptanalyst correctly guesses the key's length, then the cipher text can be treated as interwoven Caesar ciphers, which individually are easily broken.

We solve this problem by using multiplicative cipher. That's why; an intruder doesn't break the cipher text. For doing that, an intruder must know the key number then the key stream. This is quite impossible to find out two key and figure out the original message.

E. Time consumption analysis

In a network, network traffic cannot be held by the cipher. But a cipher should be helpful to do its job properly. We know, Vigenere algorithm takes a little time to scramble the message/ information. Multiplicative cipher takes a little time more than Vigenere cipher.

Individually, the algorithms take a little time. But in composition, it takes time to encrypt the data. But our

information is more valuable as we need more secure algorithm like Vigenere- Multiplicative Cipher.

F. Comparison with pros and cons

	Vigenere Cipher	Multiplicative Cipher	Vigenere-Multiplicative Cipher
Key Stream	single or multiple key	Mostly use single key	two key
Security strength	low	high	More secure
Half cipher text	No	No	Yes
Mathematical Function	Simple add function	Multiplicative inverse needed	both function needed
Time assumption	Less than multiplicative cipher	less than Vigenere-multiplicative cipher	less for same key value
Frequency analysis	sometime same cipher text for given plaintext	secure than Vigenere cipher	different cipher text for different plaintext

VII. Security Attacks [7]

When we want benefit from some resource, there should be problems to retrieve the information at risk. People benefits from the internet but there is always security attacks. The attacks may be, such as stealing the user names, passwords, credit card details, social security numbers, personal identification numbers, or any others details which can be used and have the benefits and services.

These networks and data are vulnerable to any of the following types of attacks if we do not have a security plan.

A. *Sniffing: as use of Eavesdropping*

An attacker always tries to gain the access of the information. If the data is in unsecured form, the information may be hacked. By interpreting the traffic, an intruder finds the data paths of the desired network. When an attacker is using eavesdropping on communications, it is known as sniffing or snooping.

B. *Data Modification – intruder's action*

For modification of the data, an intruder tries to find out the proper access on the network and read the information. Then the intruder can modify the data in the packet to break the confidentiality of the information.

C. *IP Address Spoofing- Routing falsely*

IP address of a computer is a valid entity to build up the trust between the networks and the operating systems. In the mean time, it is possible for an attacker to modify IP address to be falsely assumed. Most of the case, an intruder use special programs to construct IP packets that appear to originate from valid addresses inside the corporate internet. When the attacker gain the access to the network with a valid IP address, the attacker can modify, reroute, or delete data.

D. *Password-Based Attacks*

Password based attacks occurs in the operating systems and in the networks. That means our access is at risk in and out. But using proper utilization of validation we can hide our data by means of usernames and passwords.

When an attacker finds a valid user account, the intruder thinks himself as the real user. If the user has administrator-level rights, the intruder can do anything. When an intruder gains access to a network with a valid account he/she use the network falsely.

E. Denial-of-Service Attack

The denial-of-service attack prevents normal use of computer or network by valid users. The intruder tries to jam the server by creating some programs that send request to the server continuously. That's why, Normal server users find the server busy and can't gain access. These types of attack are called Denial-of Service attacks.

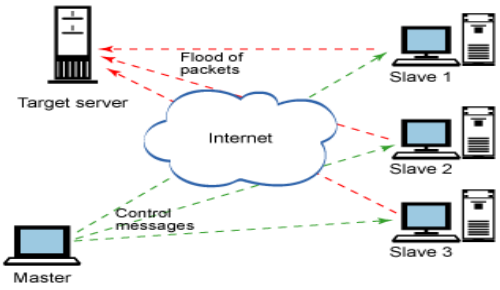

Fig. 9: Denial of service attacks

F. *Man-in-the-Middle Attack*

This type of attack is done by the intruder who is awake to monitor, capture the information which is transferred between the sender and the receiver. At the primary level of OSI reference model, it is easy for the man in the middle to find out the communication between the informer and receiver.

G. *Sniffer Attack*

In this scenario, the attacker monitors the data between the computer of the sender and the server. He collects data about the shopper or steals personal information, such as credit card numbers. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet**.**

VIII. Encryption Standards

A. *Data Encryption Standards (DES)[3]*

The most commonly used encryption programs are based on the Data Encryption Standard, which is implemented in 1977 by National Bureau of Standards (NBS) .The algorithm that is used for the data is known as Data Encryption Algorithm. It is a product cipher that operates on 64-bit blocks of data, using a 56-bit key.

The possible combination for the 2^{256} is over 72,000,000,000,000,000 keys. It is considered secured, but now days the speed of the computers increased tremendously. To break this key today's computer take very short time.

B. *Advanced Encryption Standards (AES)*

For protecting electronic data, Advanced Encryption Standards (AES) is the FIPS approved cryptographic algorithm. It is a block-cipher that encrypts and decrypts the information. By encryption process, the information is converted to an unintelligible form. At receiver point, the unintelligible form is converted to original information by decryption process. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. [6]

To perform AES algorithm, rearrangement of data and replace of data plays the important role. To rearrangement of data, we have to do permutations. Several techniques are used to do these mathematical functions. Moreover, to replace of data is called substitutions.

IX. Encryption in future: Aspect of Cryptography

From a view of technology, encryption works as operational perspective with best result. For data security, we can leave our data scrambled forever. If we do this, it will be the worst case of aspect of cryptography.

A successful enterprise security deployment will be the next target in the sense of developing encryption-decryption technique. Now, we have a problem like if a key is lost, access to all of the data originally is lost. After that, our data is totally at risk at that time. Special thought about key management should be developed. If we want to secure our electronic data with shredding, we have to create backup of the keys. [5]

X. Conclusion

An intruder always tries to retrieve the valuable information so that they can use this information falsely. Hence, computer network security with cryptography provides the remedy. Our Vigenere-Multiplicative cipher is one of our try to manage the data security with confidentiality. Hence, much more advanced security measures would be more useful. So always keep our eye on network security as it is much more important.

REFERENCES

[1] Text book Andrew s. Tanenbaum, Computer networks, fourth edition, 2003.

[2] Encryption- http://searchsecurity.techtarget.com/definition/encryption .

[3] Dr. Kamaljit I. Lakhtaria " Protecting Computer Network with Encryption Technique: A Study" published in International Journal of u- and e- Service, Science and Technology Vol. 4, No. 2, June, 2011.

[4] Text book Behrouza Forouzan, Data Communications and Networking, fourth edition, 2006.

[5] The future of Encryption http://www.net-security.org/article.php?id=1113&p=3S .

[6] Announcing the ADVANCED ENCRYPTION STANDARD (AES) Federal Information Processing Standards Publication 197 November 26, 2001.

[7] Common types of network attacks- http://www.technet.microsoft.com/en-us/library/cc959354.aspx .

[8] Comparing suitable network security http://blagovision.org/comparing-suitable-network-security-keys-kerberos-and-pki/

[9] Chey Cobb, Cryptography for Dummies the PKIPrimer, John Wiley and Sons, 2004.