ISSN: 0976-3376

Available Online at http://www.journalajst.com

ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Asian Journal of Science and Technology
Vol. 08, Issue, 03, pp.4345-4347, March, 2017

RESEARCH ARTICLE

CRYOTOGRAPHY AN OVERVIEW

***Dr. Vasundhara, S.**

Department of Mathematics, G. Narayanamma Institute of Technology and science, Shaikpet, Hyderabad, Telengana, India

ARTICLE INFO

Article History:
Received 18th December, 2016
Received in revised form
24th January, 2017
Accepted 20th February, 2017
Published online 31st March, 2017

Key words:

Cryptography,
Elgamal crptosystem,
Public key cryptography.

ABSTRACT

In this paper introducing the basic terms used in cryptography and then move on to discuss public key cryptography in more detail. We give the definitions of two public key systems, one for key exchange and one for encryption, and show how they can be adapted for use with elliptic curves. Most of the cryptographic definitions and explanations are well known and here the basics are discussed. Elgamal cryptosystems and Diffie- Hellman Cryptosystem is explained.

INTRODUCTION

In keeping with the traditions of cryptographic discussion suppose that we have two users Alice and Bob who wish to communicate securely so that the eves dropper, Eve, does not learn about the information exchanged. They will use cryptography, the science of keeping messages secure..If Alice wishes to send the plaintext, M, (her message) to Bob she will use some encryption function (E) to transform this message to cipher text, C. This cipher text should be unintelligible to any third party, but also able to be decrypted once it has been received by Bob. Plaintext −! Encryption −! Cipher text −! Decryption −! Plain text We will think of the plaintext (and cipher text) as strings of 0s and 1s (bits) which almost all messages (text, pictures etc.) can be converted into. The cryptographic algorithm that is used for encryption and decryption is known as the cipher. Restricted algorithms have security based on keeping this algorithm a secret. Such a requirement is unrealistic given any relatively large system and also allows no quality control or standardization of the algorithm. Kerchoff's assumption (1883) was that the secrecy of a cryptosystem must rely on a key and not the cipher. It is these key based systems that are used in practice, with the key space, K, defined as the range of possible keys. Increasing the key by 1 bit will double the size of the key space, so adding 5 bits for example, will make the key space 32 times bigger.

****Corresponding author: Dr. Vasundhara, S.***
Department of Mathematics, G. Narayanamma Institute of Technology and science, Shaikpet, Hyderabad, Telengana, India.

There are two main types of key-based cryptosystems:

- Symmetric key algorithms use the same key for both encryption and decryption (or the decryption key can be easily derived from the encryption key).

  EK(M) = C, DK(C) = M

Alice and Bob need to agree on this secret key before they can communicate securely.

- Public key algorithms use separate keys for encryption and decryption.

  EK1(M) = C, DK2(C) = M

The encryption key is often known as the public key and the decryption key as private. Because the encryption key is known publically, Alice does not need to have had prior communication with Bob to send him a message. A cryptosystem is an algorithm, plus all possible plaintexts, cipher texts and keys. Cryptanalysis is the attempt to obtain the plaintext without access to the key, by attacking the system. The most basic form of attack would be to try every possible key until the correct one is found which is known as a brute-force attack. It is important to make the key space large enough for this to be infeasible. However a larger key will result in more time and memory needed to perform the algorithm and so there is a trade off to consider. There are many (Fulton, 1969) other more sophisticated attacks that a

cryptanalyst can employ, which users of a cryptosystem must consider. A cryptosystem would be unconditionally secure if no matter how much cipher text an opponent has they are unable to derive the plaintext. There has only ever been one such cryptosystem, the onetime pad. This system had a key as long as the message itself, which could only be used once and so is not very practical. Most systems aim for computational security which is when the cryptosystem cannot be broken with 'available resources'. This can be defined in a variety of ways, including the amount of time, data and memory required. There are other applications of cryptography in addition to keeping messages secure that can be of great use.

These include:

- **Authentication**: A system with authentication is able to prove the origin of a message. If Bob receives a message it would be valuable to know for sure that it was sent by Alice and not some impostor.
- **Integrity**: A system with integrity would allow Bob to be sure that the message he has received has not been modified.
- **Non repudiation**: If a system provides non repudiation then Alice would not be able to falsely deny sending a message to Bob.

Public key systems, in particular, allow for these other applications .Elliptic curves are used to create public key cryptosystems which we focus on in the next section. However, at present public key systems are too cumbersome for large scale use and so messages are still encoded with symmetric key algorithms. In most industrial cryptosystems public key is used to create the key needed for the symmetric algorithm which sends the message. Since symmetrical algorithms still play such an important part we briefly look at them here. These algorithms are usually based on substitutions (swapping a bit stream for another) and permutations (rearranging the ones we have). A simple example is the Caesar cipher (used by the roman commander to communicate with his generals). Each letter is substituted for the one three Characters to the right (modulo 26).

For example:

Cryptography −! FUBSWRJUDSKB

Such a simple example could be easily broken by looking at the letter frequencies, for example. However there are much more sophisticated systems used in practice. Two such examples are the block ciphers, DES and AES.DES (the data encryption standard) was a 56-bit cipher constructed by IBM and the NSA and adopted by the USA in '76. It enjoyed wide spread use internationally but in recent years has been considered insecure for many applications. This is chiefly due to the 56-bit key size being too small; DES keys have been broken in less than 24 hours.AES (the advanced encryption standard) is a 128-bit cipher constructed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen which often goes by its creators name, Rijndael. This cipher was adopted, after a5-year standardization process, by the USA in 2001 to replace DES. Notice that the key space is substantially bigger (recall that one extra bit doubles the key space).

Public key cryptography

Public key cryptography (also known as asymmetric) uses two (Koblitz, 1994) separate keys, as opposed to symmetric encryption where the decryption key is easily derived from the encryption key. This use of two keys has profound consequences in the areas of key distribution and authentication. It should also be noted that from its earliest beginnings to modern times cryptography has been based on permutations and substitutions (from the rotor machines of WWII to complicated computer code like DES). Public key revolutionized this, basing algorithms on mathematical functions. In 1976 Walt Diffie and Martin Hellman came up with the idea of public key cryptography as a method of solving the problem of key distribution and the need for digital signatures in symmetric cryptography, by using two different but related keys for encryption and decryption. They recognized that it must be computationally infeasible to determine the decryption key given the knowledge of the cryptographic algorithm and encryption key. Figure1.1 demonstrates how such a system would allow Alice to securely send a message to Bob without any prior contact. Some algorithms will also have the property that either of the two keys can be used for encryption with the other used for decryption. In this case the public key algorithm could be used for authentication as in Figure 1.2. In addition to knowing the message could only have come from Alice Bob can also be sure of the data security as no-one without access to Alice's private key could have altered the message.

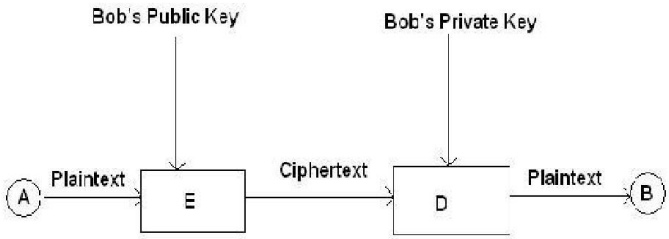

Figure 1.1

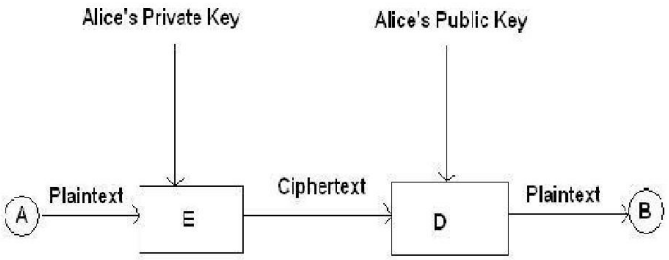

Figure 1.2.

Public key authentication: Alice encrypts a message with her private key and sends it to Bob. Only Alice could have sent the message as only she has access to the private key necessary for encryption. The authenticated message could be read by anyone who has access to Alice's public key, so it must also be encrypted with Bob's public key to be secure. To be more efficient Alice should only encrypt a small segment with her private key for authentication purposes (an authenticator block) and then encrypt the whole message in Bob's public key. Diffie & Hellman recognized the possible uses of such a public key cryptosystems:

- **Encryption / decryption:** The sender encrypts a message with the recipient's public key.
- **Digital signature:** The sender signs a message with his public key.
- **Key exchange:** Two sides cooperate to exchange a session key.

Although postulating this system, Diffie & Hellman did not demonstrating that such an algorithm for encryption exists Diffie & Hellman also recognized the need for a trapdoor one-way function in such a system. A one-way function maps a domain so every function value has a unique inverse, with the condition that the calculation of the function value is easy where as the calculation of the inverse is infeasible. (Easy implies polynomial length computation time.) A trapdoor one-way function is the same except that the inverse is easy to compute if certain additional information is known. Therefore we require a function f such that:

Y = fk(X) is easy to compute, if k and X are known
$X = f^{-1}$
k (Y) is easy to compute, if k and Y are known
$X = f^{-1}$

k (Y) is infeasible to compute, if Y is known but k is not The classic example of such a function is the factorization of large primes modulo p. While it is relatively easy to multiply the two primes it is extremely difficult to factorise the product, unless some other information is known. The first successful algorithm for public key encryption was RSA in 1978, named after its creators Ron Rivest, Adi Shamir and Len Adleman. This system relied on the prime factorization problem described above and has since been widely used in a variety of applications. Although an important subject in cryptography it is not used in conjunction with elliptic curves and so not discussed here. As with symmetric schemes, the security of a public key system depends on the size of the key, and any algorithm would be vulnerable to a brute force attack of trying all possible keys. The countermeasure is to use large keys, however unlike symmetric schemes the computation time may not rise linearly with the key size and so there is a tradeoff between security and practicality. In practice the key sizes that make brute force attacks impractical result in encryption speeds that are too slow for general use. This is why, as mentioned earlier, public key cryptography has been confined to key management and signature applications, and such as key exchange and authentication the actual message to be transferred is then encoded with a symmetric key system (eg AES). Due to the level of computation involved in public key systems this is likely to remain the case for some time with Walt Diffie himself saying, 'the restriction of public key cryptography to key management and signature applications is almost universally accepted'.

The El Gamal Cryptosystem

This is a public key cryptosystem based on the discrete log problem, first proposed in 1984. It will allow Alice to securely send a message to Bob without prior communication. This description of the El Gamal system was [ ] assume the message can be stored as an element of Z^*_p and define the algorithm as follows.

The key is formed from the prime p, the primitive root α an integer a and $\beta = \alpha^a \pmod p$. The values p, a,α β are made public while a is kept private. If Alice wants to send a message, $M \in \{0, 1, ..., p - 1\}$, to Bob she proceeds as follows.

- Alice selects a random integer $r \in Z^*_p$.
- Alice computes $y_1 = \alpha^r \pmod p$ and $y_2 = M\beta^r \pmod p$.
- Alice sends the cipher text C = (y1, y2) to Bob.
- Bob uses his private key, a, to calculate $y_2\ y_1^{p-1-a} \pmod p$ which givescthe message M.

The decryption in the final step works because

$y_2\ y_1^{p-1-a} = y_2\ y_1^{-a} 1$ since $x^{p-1} \equiv 1 \pmod p$
$= (m\beta^r)(\alpha^r)^{-a}$ by the definition of y_1 and y_2
$= m(\beta^r)(\alpha^{-ar}) = m(\alpha^{ar})(\alpha^{-ar}) \equiv m \pmod p$

Any third party would know p, α,β, $y_1 = \alpha^r$ and $y_2 = m\beta^r$. To recover m a third party could attempt to solve the discrete logarithm problem and find a from $\beta = \alpha^a$. If the problem is set up carefully then this is considered infeasible. It is important that Alice use a different random integer each time she sends a message. Suppose the same r was used to encrypt both m1 and m2and the resulting cipher text were (y_1, y_2, (z_1, z_2). Then

$$\frac{y_2}{z_2} = \frac{m_1\beta^r}{m_2\beta^r} = \frac{m_1}{m_2}$$

Then suppose that the secret message m1 was made public at some later point. If this happened then anyone who had stored the cipher text could easily compute the new secret message m2 by calculating $\frac{m_1 z_2}{y_2} = m_2$. Even worse, the eves dropper can easily recognise that this mistake had been made as y_1 would equal z_1.

REFERENCES

Archbold, J. W. 1970. Algebra, Fourth Edition, Pitman Paperbacks, 1970.

Cohen, H., G. Frey, 2006. Handbook of elliptic and hyper elliptic curve cryptography, Chapman & Hall/CRC.

Course notes - MT362 Cipher systems, Royal Holloway University of London, 2004

Fraleigh, J. B. 1994. A first course in abstract algebra, 5th edition, Addison-Wesley.

Fulton, W. 1969. Algebraic curves, W. A. Benjamin, Inc.

http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm?MenuID=10.2.777.

Koblitz, N. 1994. A course in number theory and cryptography, Springer.

Levy, S. 2000. Crypto, Allen Lane.

NSA website: The case for elliptic curve cryptography.

Schneier, B. 1996. Applied cryptography, Second Edition, John Wiley.

Stallings, W. 2003. Cryptography and network security, Third Edition, Prentice Hall.

Washington, L. C. 2003. Elliptic curves, Chapman & Hall/CRC.

****