ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 5, Issue, 01, pp.054-055, January, 2013

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

Applications of Quantum Cryptography

[1]Vijayalakshmi, C., [2]Palaniammal, S. and [3,*]Ramya, K.

[1]Department of Mathematics, VIT University, Chennai India
[2]Department of Mathematics Sri Krishna College of Engineering, Coimbatore, India
[3]Department of Mathematics, Kingston Engineering College, Vellore

ARTICLE INFO

Article History:
Received 02th October, 2012
Received in revised form
19th November, 2012
Accepted 26th December, 2012
Published online 16th January, 2013

Key words:
Algorithms,
Mathematical explanations,
Modular arithmetic,
Quantum mechanics,
Data Encryption.

ABSTRACT

This paper deals the public key cryptography and Quantum cryptography and its uses in the applications such as Key Agreement, Data Encryption and Digital Signature. This paper discusses some public key algorithms, mathematical explanations on the working of these algorithms and also gives a brief introduction to modular arithmetic, which is the core arithmetic of almost all public key algorithms. Quantum cryptography could well be the first application of quantum mechanics at the single-quantum level.

INTRODUCTION

Electrodynamics was discovered and formalized in the 19th century. The 20th century was then profoundly affected by its applications. The most peculiar characteristics of quantum mechanics are the existence of indivisible quanta and of entangled systems. Both of these lie at the root of quantum cryptography (QC), which could very well be the first commercial application of quantum physics at the single quantum level. In addition to quantum mechanics, the 20th century has been marked by two other major scientific revolutions: information theory and relativity. The data transferred from one system to another over public network can be protected by the method of encryption. On encryption the data is encrypted by any encryption algorithm using the 'key'. Only the user having the access to the same 'key' can decrypt the encrypted data. This method is known as private key or symmetric key cryptography. There are several standard symmetric key algorithms defined

One-Way function

In public key cryptography, keys and messages are expressed numerically and the operations are expressed mathematically. The private and public key of a device is related by the mathematical function called the one-way function. One-way functions are mathematical functions in which the forward operation can be done easily but the reverse operation is so difficult that it is practically impossible. In public key cryptography the public key is calculated using private key on the forward operation of the one-way function. Obtaining of private key from the public key is a reverse operation. If the reverse operation can be done easily, that is if the private key is obtained from the public key and other public data, then the public key algorithm for the particular key is cracked. The reverse operation gets difficult as the key size increases. The public key algorithms operate on sufficiently large numbers to make the reverse operation practically impossible and thus make the system secure. For e.g. RSA algorithm operates on large numbers of thousands of bits long.

Public -key cryptosystems

Cryptosystems come in two main classes—depending on whether Alice and Bob use the same key. Asymmetrical systems involve the use of different keys for encryption and decryption. They are commonly known as *public-key cryptosystems*. Their principle was first proposed in 1976 by Whitfield Diffie and Martin Hellman, who were then at Stanford University. The first actual implementation was then developed by Ronald Rivest, Adi Shamir, and Leonard Adleman of the Massachusetts Institute of Technology in 1978. 4 It is known as RSA and is still widely used. If Bob wants to be able to receive messages encrypted with a public-key cryptosystem, he must first choose a private key, which he keeps secret. Then he computes from this private key a public key, which he discloses to any interested party. Alice uses this public key to encrypt her message. She transmits the encrypted message to Bob, who decrypts it with the private key. Public-key cryptosystems are convenient and have thus become very popular over the last 20 years. The security of the Internet, for example, is partially based on such systems. They can be thought of as a mailbox in which anybody can insert a letter. Only the legitimate owner can then recover it, by opening it with his private key.

Algorithms and Explanations

This section discusses a few public key algorithms and also gives an explanation on how these algorithms work. The algorithms covered in this section are

- Key Agreement Algorithms – RSA, DH, ECDH
- Encryption Algorithms – RSA
- Signature Algorithms – RSA, DSA, ECDSA

Corresponding author: Ramyadasan@yahoo.co.in

Modular Arithmetic

Modular arithmetic deals only with integers. Since it involves no floating-point operations, the mathematical calculations are more accurate and efficient than the real number arithmetic. Modular arithmetic over a number n involves arithmetic operations on integers between 0 and n – 1, where n is called the modulus. If the number happens to be out of this range in any of the operation the result, r, is wrapped around in to the range 0 and n – 1 by repeated subtraction of the modulus n from the result r. This is equivalent in taking the remainder of division operation r/n.

For example for modulo 23 arithmetic
n=23, Let a=15, b=20
(a+b) mod n = (15+20) mod 23 = 35 mod 23 = 12

Since the result of a+b=35 which is out of the range [0,22], the result is wrapped around in to the range [0 22] by subtracting 35 with 23 till the result is in range [0,22]. a mod b is thus explained as remainder of division a/b. Subtraction and multiplication can also be explained similarly. A negative number is added repeatedly with n till it can be represented in the range [0,n-1] The modular division a/b mod p is defined as a*b-1 mod p. b-1 is the multiplicative inverse of b.

Congruent relation

Modular arithmetic is a congruent relation. Congruence is shown by the symbol '≡'. For a modulus n two numbers a and b are said to be congruent if a mod n ≡ b mod n.

i.e. a ≡ b (mod n) if, a mod n = b mod n

For example consider the modulus 7
i.e. n = 7
Then the numbers 2, 9, 16, 23 etc are congruent to each other since (2 mod 7) = (9 mod 7) = (16 mod 7) = (23 mod 7) etc

Properties of modular arithmetic

1. a≡b mod n implies a–b=k*n, where k is an integer
2. a mod n + b mod n ≡ a+b (mod n), also true for other operators '-', '*'and '/'
3. a+b≡b+a (mod n) , also true for other operators '-', '*'and '/'
4. a≡a mod n
5. a≡b mod n implies b≡a mod n
6. Fermat's little theorem, if M and p are coprime then Mp-1≡1 (mod p)
7. If p and q are co-prime and also if a≡b(mod p) and a≡b(mod q) then a≡b(mod pq)

Elliptic Curve Cryptography(ECC)

Elliptic curve cryptography (ECC) is relatively new technology compared to other public key cryptography such as RSA. Elliptic key operates on smaller key size. A 160-bit key in ECC is considered to be as secured as a 1024 bit key in RSA. ECC operates on the points in the elliptic curve y2=x3+ax+b, where 4a3+27b2≠0. The above equation of elliptic curve is in real coordinate. To make elliptic curve operation efficient and accurate the elliptic curve can be defined in finite fields. Elliptic curve in two finite fields, prime field and binary field, are defined by standard. In prime field operation the elliptic curve equation is modified as y2mod p=x3+ax+b mod p, where 4a3+27b2 mod p≠0. The ECC standards are specified in SEC, Standards for Efficient Cryptography

Domain parameters

There are certain public constants that are shared between parties involved in secured and trusted ECC communication. This includes curve parameter a, b, a generator point G in the chosen curve, the modulus p, order of the curve n and the cofactor h. There are several standard domain parameters defined by SEC, Standards for Efficient Cryptography

Point multiplication

Point multiplication is the central operation in ECC. In point multiplication a point A on the elliptic curve is multiplied with a scalar k using elliptic curve equation to obtain another point B on the same elliptic curve.
i.e. k*A=B

Point multiplication is achieved by two basic elliptic curve operations

• **Point addition**, adding two points X and Y using elliptic curve equation to obtain
another point Z i.e., Z = X + Y.

• **Point Doubling**, adding a point X to itself using elliptic curve equation to obtain
another point Z i.e. Z = 2X.

Here is a simple example of point multiplication. Let P be a point on an elliptic curve. Let k be a scalar that is multiplied with the point P to obtain another point Q on the curve.

i.e. Q = k*P.
If k = 23 then k*P = 23*P = 2(2(2(2P) + P) + P) + P.

In the ECC explanations given below upper case letter indicates a point in the elliptic curve and the lower case letter indicates a scalar

One Way function in Elliptic Curve Cryptography

The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem. Let A and B be two points on an elliptic curve such that k*A = B, where k is a scalar. B can be easily obtained from A and k but given A and B, it is computationally infeasible to obtain k, if k is sufficiently large. k is the discrete logarithm of B to the base A.

Conclusion

Cryptography is used frequently. For example, credit card numbers are encrypted when you buy something on the internet. Many government agencies are used cryptography to get messages safely around the world. Public key cryptography is an innovation and which is an unavoidable part of almost all security protocol and application. Being able to negotiate a shared secret between two devices online without the need of any exchange of secret data created a breakthrough in secure network/internet communication.

REFERENCE

FIPS PUB 186-2, *Digital Signature Standard (DSS),* January 2000
Bechmann-Pasquinucci, H., and A. Peres, 2000, ''Quantum cryptography with 3-state systems,'' Phys. Rev. Lett. 85, 3313–3316.
Ekert, A. K., 1991, ''Quantum cryptography based on Bell's theorem,'' Phys. Rev. Lett. 67, 661–663.
Ekert, A. K., 2000, ''Coded secrets cracked open,'' Phys. World

****