Public-key cryptography term papers example

Science, Mathematics

General definition

Public-key algorithm of cryptography, sometimes names as asymmetric cryptography. It is a class of cryptographic algorithms which uses two separate keys, one of which is known only by one side (secret or private) another one is available for publicity (public).

These 2 keys are different, but they are connected with some mathematical operations. The public key is usually used to encrypt(code) data or to verify and confirm a digital signature. The private key is used to decode (decrypt) data or to create a digital signature.

The term asymmetric describes this algorithm because different keys are used to run the opposite functions. Each operation is the inverse of the other. This principle comes in opposite with conservative (symmetric) approach to cryptography. Regular cryptography usually is based on the same key and function to run both coding and decoding of information.

Public-key cryptography algorithms rely on mathematical tasks, which do not have fast(good) solution (means there are no solution in at least polynomial time. Very often, such problems are NP questions). Such problems usually include operations like logarithm, heavy calculations(factorial) or elliptic relationships, etc. It is easy(able to compute fast) to create public and private key-pair and use them for coding and decoding(encryption and decryption).

The main strength of the algorithm is the fact that it is very hard and almost " impossible" (computationally infeasible) to determine generated private key from the public one. The public key could be shared without security issues (concerns), on the other hand, the private key should be hidden from

anyone without permission to read messages or use digital signatures.

Another advantage is that public key algorithms do not require previous secure exchange of secret keys between the participants of messaging.

Lets look at public key algorithm in more details.

Let be a space of keys, and — encryption and decryption keys respectively. — encryption function for a random key where :

Here , where is a space of encrypted messages, , where — space of messages.

— decryption function which allows us to find message , from encrypted text :

{: } — encryption set, a {: } — decryption set respectively.

Each pair has a property: if we know , we cannot solve equation , so for a random encrypted text , message cannot be found.

This means that given is not enough to determine decryption key. - one side function.

Lets look at public key algorithm example to receive a better understanding of how it works.

Two numbers are considered to be congruent in modulus arithmetic if their difference is divisible by the modulus[2]. For example, 51 is congruent to 2 modulus 7 because the difference between 2 and 52 is divisible by 7.

Congruency can be expressed in different way. Consider a≡b(modm) if a= zm+b where z is an integer.

- Bob is going to receive coded message from Alice

- Everyone can encrypt the message.

- ONLY Bob can decrypt message.

Bob chooses two (very large) prime numbers p and q, and calculates n, n= pq.

After it n is used to encrypt the message. It is important that p and q are needed to decrypt the coded message.

- Bob chooses two big (distinct) prime numbers p and q;

- n= pq, m= lcm {p−1, q−1} (the least common multiple of p and q);

- Bob determines r, where r> 1 and r is coprime with m (r and m have no common factors);

- Bob calculates the unique s, rs≡1(modm)

- Bob makes n and r public, but does NOT give p, q or s.

- Alice tries to send Bob the message M (represented by a number) where M and n are coprime, 0 - Alice finds Mc, Mc≡M^r(modn), and sends it to Bob.

- Bob receives encrypted message Mc from Alice and decrypts it.

Bob knows p, q, m, n, r, s. He uses these to decrypt the message Mc from Alice. Bob uses (Mc)^s≡M(modn) theorem to find M. Lets consider practical example to receive full understanding of how the algorithm works.

- Alice wishes to send the message M to Bob

- Bob picks p= 2, q= 3; so n= 6, m= 2, r= 3 and s= 5.

- Bob gives Alice n= 6 and r= 3.

- Note: It does not matter how many people have this information, they still won't be able to find s.

- Alice calculates Mc and determines Mc= 15.

- Bob gets the coded data 180 from Alice

- Bob make calculations M≡15^6(mod6), and decode the message M.

- M = 3 [1].

References:

- Beardon, T. (n. d.). Public Key Cryptography. Retrieved December 2, 2014, from http://nrich. maths. org/2200

- Public Key Encryption and Digital Signature: How do they work? (n. d.). Retrieved December 2, 2014, from http://www. cgi. com/files/white-papers/cgi_whpr_35_pki_e. pdf

- Katz, Jon; Lindell, Y. (2007). Introduction to Modern Cryptography. CRC Press. ISBN 1-58488-551-3.