International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 02 | Feb - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Public Key Encryption Using Key Generation

DR C.P. Indhumathi Assistant prof Bharathidasan Institute of Technology Campus, Anna University,
Prof Dr. Brindha Tirugnanasambandam1 Associate prof M.A.M School of Engineering Siruganur , Trichy 105

Abstract: Public key encryption with key word search enables a sender to receiver to send message with security concern with semantic security with computational complexity with related to information retrieval in the private database with key generation run by the receiver takes a security parameter as input and generates a public or private key pair is discussed in this paper

Key words: Encryption, Decryption, digital signature, public key encryption, private key encryption

The department of Science and technology provides security architecture provides a systematic framework for defining security attacks mechanisms and services. It is designed to detect security mechanism to detect prevent or recover from a security attack. The key components of secure communication are confidentiality authentication message Integrity and non-repudiation. Through a continuous cycle of protection detection and response network security is achieved. Through an active Intruder we can remove messages from the channel and or add messages into the channel. Recording the control and data messages is done on passive intruder. The principle of confidentiality ensures only sender and recipient have to have access to message.

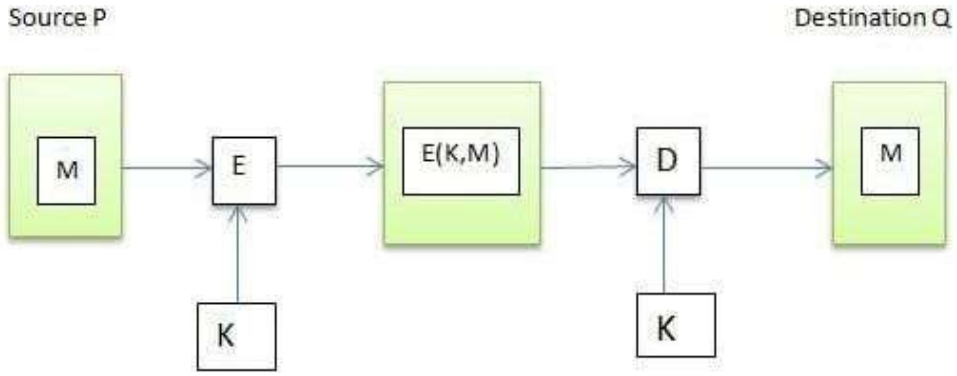
The security mechanism are confidentiality authentication Integrity non-repudiation access control and availability. A security policy is good generally takes care of four aspects of affordability functionality legality and cultural issue

Authentication function Functions at lower level produce an authentication. This value is used to authenticate this value is used to authenticate a message.
The lower-level function is used in higher level protocol that is authentication protocol
enables receiver to verify authenticity of message. Following are the three types of functions Message encryption
Message authentication Hash function Message encryption
Ciphertext of the entire message serves authenticator message encryption by itself provide message measure of authentication

Symmetric encryption

The message encryption is symmetric encryption

A message M transmitted from A to B encrypted using secret key K shared by A and B. If no other party knows the key, then confidentiality is provided.

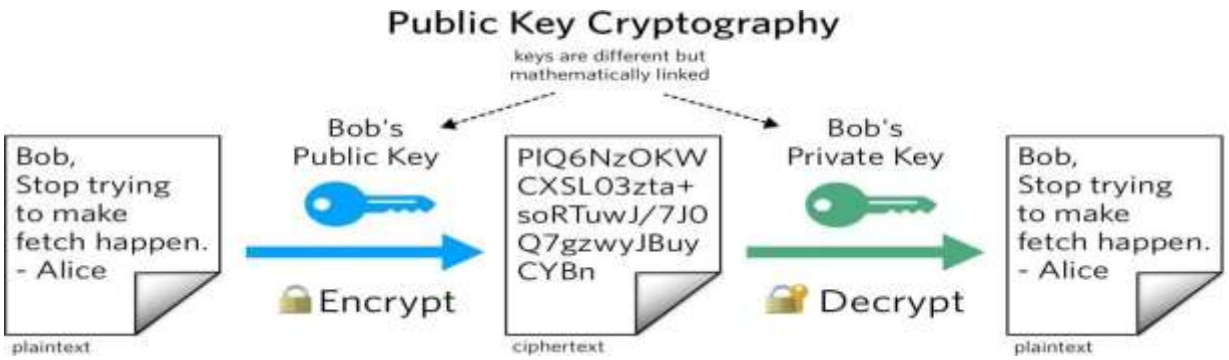


Symmetric encryption is confidentiality and authentication, P generates message To destination Q. Both party uses secret key provide authentication and confidentiality.

A function D decrypts and a secret key K is generated from input X produces output by D (K, x) Let X Cipher text of message corresponding encryption function plain text for message M thus y produces meaningless sequence of bits.

Public key encryption

Public encryption provides confidentiality but not authentication.



PUb is public key of Destination B to for Source A a and corresponding private key PRb. The public key encryption, to encrypt a message A, provides no authentication. For Encryption to encrypt a message a provides no authentication. For encryption of the message A uses a private key PRA B uses a public key to decrypt it gives a process also Provide digital signature.

To provide authentication confidentiality a encrypts message using private key also provides digital signature then using B public key.

MAC Message authentication code Secret key is used by message authentication code. The two parties share a same common key secret key. A sends a message to B it calculates MAC is equal to C of K, m is the input message C is the Mac function

Key is the shared secret key.

Mac message authentication code. Receiver transmits the message calculated by message authentication code.

The receiver transmits calculated Mac and message Mac is calculated.

1 Receiver is assured That message has not been altered

2 The receiver is assured that messages are from alleged sender

Here we have Digital signature Cyberworld having a sort of dual signature replacing handwritten signatures is essential in the cyber world. It is important between two parties who do not trust each other and need protection from each other's later false claims. The legal documents are authenticated financial documents are authenticated with handwritten digital signature. For computerized message systems to replace physical transport of paper and Link document solution must be found to this problem. Must authenticate the content of message at the time of signature. Authentication is the process of determining private or public computer networks.

Conclusion: In this paper we have highlighted about public key cryptography proven to security model in multi-user setting.

References

[1] Bai, L., Yong, L., Chen, Z., and Shao, J. (2024). Pairingfree public-key authenticated encryption with keyword search. Computer Standards & Interfaces,

88:103793.

[2] Huang, Q., Huang, P., Li, H., Huang, J., and Lin, H. (2023). A more efficient public-key authenticated encryption scheme with keyword search. Journal of Systems Architecture, 137:102839.

[3] Huang, Q. and Li, H. (2017). An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks. Information Sciences, 403:1–14.

[4] Lu, Y. and Li, J. (2022). Lightweight public key authenticated encryption with keyword search against adaptively-chosen-targets adversaries for mobile devices. IEEE Transactions on Mobile Computing, 21(12):4397–4409

Dr C.P Indhumathi Assistant prof (Sr grade) is working as Asistant prof (Sr grade) Bharathidasan Institute of Technology Campus, Anna University, Tiruchirappalli has Research Area in Software Engineering, Software Testing, Optimization Techniques , Object Oriented Design Patterns , UI/UX Design Concepts Software Defined Network is having 15 years of experience

Authors Dr T.Brindha is currently working as an Associate professor in M.A.M School of Engineering for Computer Science Department, Artificial Intelligence and Data Science, Trichy, Tamil Nadu, INDIA. Her interested areas include Data Base and Management Systems, Computer Networks, Object Oriented Analysis and Design, Artificial Intelligence, Big-Data, Cloud Computing, Python, Bio-informatics. She has publications in reputed journals and conferences.