# Report on public key encryption

Technology, Information Technology

Public Key Encryption The world has become electronic in almost all its activities. Therefore, there is need to provide an identifier for online users. As a result, the public key encryption provides an identity to the world. This mainly affects those who seek to find data or information online. Moreover, technology needs to be secure to avoid fraudsters from tampering with vital information. Consequently, people need a passport or identification to access online information. However, public key encryption makes use of long numbers. These numbers are known as keys (Ferguson & Schneier, 2003 p18). The process becomes more secure when the numbers are longer. There are two keys and they include the private and public keys. For example, the smartcard and a padlock for the private and public keys, respectively.

Logically, any individual can access the public keys. However, the two types of keys work together. This paper, therefore, provides a detailed report on Public Key Encryption.

Alice (public key) Kevin (private key)

Combined key 12345678 (shared secret between Alice and Kevin)

The above diagram shows that with the keys as identity, the two can share data or information.

For example, Kevin could send Alice important data that he wants to ensure only she gets to read it. Therefore, Kevin encrypts the data with Alice’s public key since only Alice knows this public key hence she alone can encrypt the data in its original form.

An individual needs to prove that he or she owns the identity when they are online. This is because the document needs to recognize the identity of the

user in order to know the person (Paar & Pelzl, 2010 p152). In addition, the keys help in coding of data. For instance, the message is applied to a publicly known mathematical hashing function that coverts the message in to a long number referred to as the hash. This is because the hash is part of the document that is signed to a user (Paar & Pelzl, 2010 p293). Consequently, when data has been scrambled using a private key, it is unscrambled using the public key. The reverse also happens when the private key is used to unscramble. This is done using another hash that is obtained from the data.

Alice

Large numbers in random order

Key generate process

Public key private key

This diagram above shows that the two keys work together when data is scrambled

In conclusion, the public key encryption aids the protection of data or information. Therefore, an individual signs in using a number of keys. The keys are what the data uses to check the identity of the person. As a result, the keys act as a signature of verification for online users.

Bibliography

Ferguson, N., & Schneier, B. (2003). Practical cryptography. Indianapolis, Ind, Wiley.

Paar, C., & Pelzl, J. (2010). Understanding cryptography: a textbook for students and practitioners. Berlin, Springer.