### TEXT ENCRPYTION USING VARIOUS ALGORTHIMS

CASE STUDY:

Data security involves techniques of communicating in a secret manner in such a way that valuable

information is kept sacrosanct from unauthorized users In order to ensure this secret communication, many cryptographic schemes have been developed over the years with different number of keys, and levels of encryption and decryption. The sole objective of such schemes is to make it difficult for untended persons online of communication to have access to the information or message and/or if they ever did, then it should be very difficult for such persons to decode the content of the transmitted message.

However, the degree of security offered by a cryptographic scheme depends to a larger extent on the type and length of the keys utilised, the levels of encryption to create chaos, the throughput rate of the algorithms as well as the ability of such encryption algorithms to encrypt smaller messages, Encryption involves translating the

Kalpa Publications in Computing

Volume 12, 2019, Pages 20–31

Proceedings of 4th International Conference on the

Internet, Cyber Security and Information Systems 2019

original message (usually in plaintext) into a cypher text using an encryption key. The reverse process

of getting back the plaintext (message) from the cypher text (also with a decryption key) is termed

decryption

There are three major types of cryptography namely symmetric, asymmetric and hash functions.

Symmetric cryptography uses a single key for both encryption and decryption. The asymmetric

cryptography uses two keys; one for encryption (known as the public key), and the other for decryption

(known as private key). The final class, Hash Functions use no key but compute a fixed-length

mathematical irreversible hash value based on the plaintext that makes it impossible for either the

contents or length of the plaintext to be recovered Popular amongst the cryptographic schemes are the Data Encryption Standards (DES) and Advance Encryption

Standards (AES) for single key cryptography and the Rivest, Shamir and Adleman (RSA) for double

key cryptography. However, these schemes have been susceptible to cryptographic attacks such as brute

force attacks in the case of DES and AES, and computational attacks on the RSA

QUESTIONS AND ANSWERS FRAMING:

1) Difference between aes and des algorthim?

|  |  |
| --- | --- |
| *AES* | *DES* |
| AES stands for Advanced Encryption Standard | *DES stands for Data Encryption Standard* |
| The date of creation is 1999. | *The date of creation is 1976.* |
| Byte-Oriented. | *Bit-Oriented.* |
| Key length can be 128-bits, 192-bits, and 256-bits. | *The key length is 56 bits in DES.* |
| Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits) | *DES involves 16 rounds of identical operations* |
| The structure is based on a substitution-permutation network. | *The structure is based on a Feistel network.* |
| The design rationale for AES is open. | *The design rationale for DES is closed.* |
| The selection process for this is secret but accepted open public comment. | *The selection process for this is secret.* |
| AES is more secure than the DES cipher and is the de facto world standard. | *DES can be broken easily as it has known vulnerabilities. 3DES(Triple DES) is a variation of DES which is secure than the usual DES.* |
| The rounds in AES are: Byte Substitution, Shift Row, Mix Column and Key Addition | *The rounds in DES are: Expansion, XOR operation with round key, Substitution and Permutation* |
| AES can encrypt 128 bits of plaintext. | *DES can encrypt 64 bits of plaintext.* |
| AES cipher is derived from an aside-channel square cipher. | *DES cipher is derived from Lucifer cipher.* |
| AES was designed by Vincent Rijmen and Joan Daemen. | *DES was designed by IBM.* |
| No known crypt-analytical attacks against AES but side channel attacks against AES implementations possible. Biclique attacks have better complexity than brute force but still ineffective. | *Known attacks against DES include Brute-force, Linear crypt-analysis, and Differential crypt-analysis.* |

2)The best time complexity for encryption and decryption algorithm according to the case study?

ANS: Although, the time complexity of AES, DES, 3DES, RC4 and BlowFish and most of the cryptographics algorithms is O(k), where k is a constant that actually depends upon the underlaying harware used for encryption.

But according to the case study AES algorithm is the trusted standard algorithm used by the United States government, as well as other organizations. Although extremely efficient in the 128-bit form, AES also uses 192- and 256-bit keys for very demanding encryption purposes. AES is widely considered invulnerable to all attacks except for brute force. Regardless, many internet security experts believe AES will eventually be regarded as the go-to standard for encrypting data in the private sector.

3) What is the Symmetric Encryption Method?

It’s Also called as private-key [cryptography](https://www.simplilearn.com/understanding-cryptography-article) or a secret key algorithm, this method requires the sender and the receiver to have access to the same key. So, the recipient needs to have the key before the message is decrypted. This method works best for closed systems, which have less risk of a third-party intrusion. On the positive side, symmetric encryption is faster than asymmetric encryption. However, on the negative side, both parties need to make sure the key is stored securely and available only to the software that needs to use it.

4)What is the Asymmetric Encryption Method?

Also called public-key [cryptography](https://www.simplilearn.com/understanding-cryptography-article), this method uses two keys for the encryption process, a public and a private key, which are mathematically linked. The user employs one key for encryption and the other for decryption, though it doesn’t matter which you choose first.

*IMPLEMENTING IP ADDRESSING SCHEME USING IPV6*

*CASE STUDY:*

As a communication protocol, IP provides an identification and location system for computers on the Internet. Internet Protocol version 4 (IPv4) has been used successfully for the past years. As the successor of IPv4, Internet Protocol version 6 (IPv6) was developed by the Internet Engineering Task Force (IETF) since 1998. Currently, IPv4 still routes most Internet traffic [4]. However, due to the predictable exhaustion of IPv4 addresses [5], the transition to IPv6 is imperative, because, compared with IPv4, IPv6 can provide a larger available address space.

To try and encourage the adoption of IPv6, more than 400 organizations and institutions participated in the Word IPv6 Day on 8th June 2011 [To further promote the deployment and development of IPv6, World IPv6 Launch was held on 6th of June 2012 Google has announced that over 10% of users access Google through IPv6 CAIDA has shown that, from January 2014 to January 2015, the number of IPv6 ASes increased by 23% and the number of links between them increased by 29% Existing studies have addressed that IPv6-centric next generation networks are widely deployed and applied With the development of IPv6, applications such as video conference, IPTV, VoIP, and online games will become more and more prevalent in IPv6 networks, so keeping network availability as well as good performance is crucial. Investigating the performance of IPv6 network is the basis of guaranteeing the network with a good performance. Therefore, many studies have been performed to analyze IPv6 network performance, as well as figure out the differences between IPv4 and IPv6 However, our understanding of IPv6 network cannot catch up with the speed of its development. A revisiting of current IPv6 network performance is needed.

QUESTIONS AND ANSWERS FRAMING:

1)What is the size of an IP address in IPv6?

All IPv6 addresses are **128 bits** long, written as 8 sections of 16 bits each. They are expressed in hexadecimal representation, so the sections range from 0 to FFFF

2) what is ipv6 address scope?

Unicast and multicast IPv6 addresses support address scoping, which identifies the application suitable for the address.

Unicast addresses support global address scope and two types of local address scope:

Link-local unicast addresses—Used only on a single network link. The first 10 bits of the prefix identify the address as a link-local address. Link-local addresses cannot be used outside the link.

Site-local unicast addresses—Used only within a site or intranet. A site consists of multiple network links. Site-local addresses identify nodes inside the intranet and cannot be used outside the site.

Multicast addresses support 16 different types of address scope, including node, link, site, organization, and global scope. A 4-bit field in the prefix identifies the address scope.

3 )Which web sites use IPV6?

There are now numerous web sites that are connected using IPV6. If you are looking for a web site to test your IPV6 connectivity to or just curious about which sites you may already be visiting over IPV6 transport, there are many to choose from. The most popular IPV6-connected web sites are Google.com, YouTube.com, Linkedin.com, Facebook.com, Instagram.com, Wikipedia.com, Netflix.com,

Blogspot.com, Apple.com, among many others.