ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 3, pp: (68-70), Month: July - September 2021, Available at: www.researchpublish.com

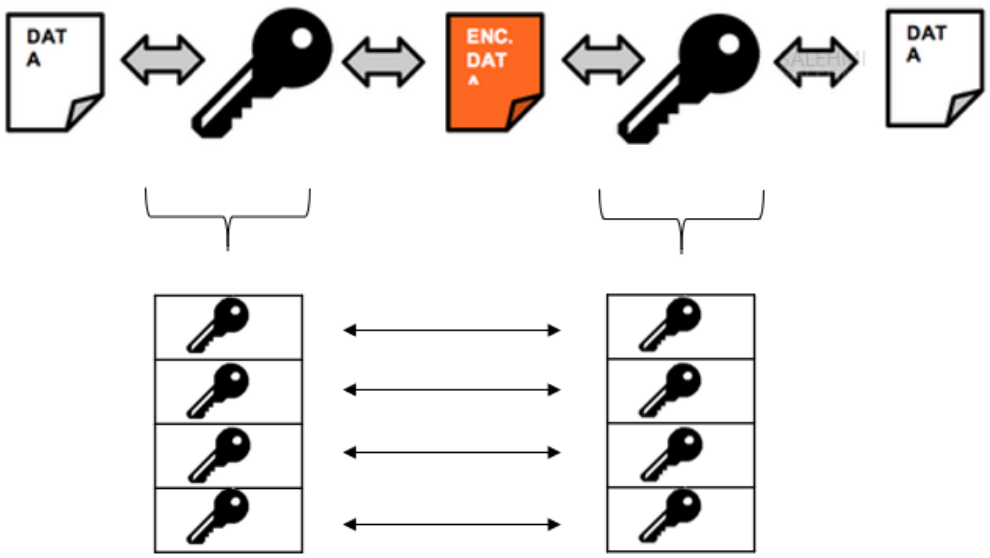
# TLS symmetric key exchange from single key to multiple keys for enhanced security

[1]Mashael Alsaleh, [2]Abdullah aldossary

***Abstract:*** **TLS is a broadly deployed protocol over IP networks for providing a secure channel between two communicating hosts, typically a client and a server to prevent eavesdropping, message forgery and tampering. Moreover, TLS regular symmetric is dependent on one key for encryption and decryption. While In this invention, TLS symmetric key exchange uses multiple keys on both sides of the conversation, for both encrypting and decrypting to enhance the security and data integrity over internet communications. This invention will enhance the security of the TLS encryption and protect against single symmetric key compromise.**

***Keywords:*** **TLS symmetric, multiple keys, TLS encryption. enhanced security.**

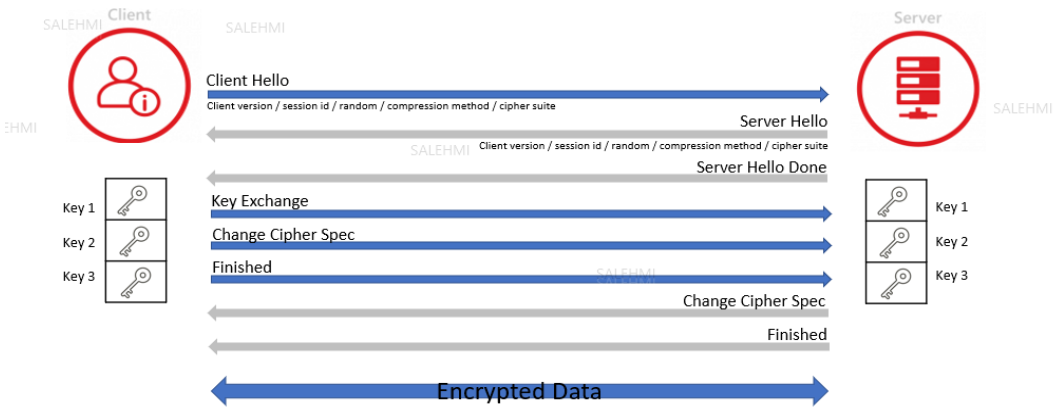
## 1. INTRODUCTION




TLS is a broadly deployed protocol over IP networks for providing a secure channel between two communicating hosts, typically a client and a server to prevent eavesdropping, message forgery and tampering. Moreover, TLS regular symmetric is dependent on one key for encryption and decryption. While In this invention, TLS symmetric key exchange uses multiple keys on both sides of the conversation, for both encrypting and decrypting to enhance the security and data integrity over internet communications. This invention will enhance the security of the TLS encryption and protect against single symmetric key compromise.

In this Research, Tls uses symmetric cryptography. The data is encrypted and decrypted with multiple of keys known to both server and client.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 3, pp: (68-70), Month: July - September 2021, Available at: www.researchpublish.com




**Step 1: Client Hello (Client → Server)**

First, the client sends a Client Hello to the server. The Client Hello includes the following information Like (Client version, Client Random, Session ID, compression methods, Cipher Suite, Compression Methods, Extension)

**Step 2: Server Hello (Server → Client)**

After the server receives the Client Hello, it replies with a Server Hello. A Server Hello may either contain selected options like( server version, server Random, Session ID, compression methods, Cipher Suite, Compression Methods, Extension) or it may be a handshake failure message.

**Step 3: Server Certificate (Server → Client)**

The server now sends a signed TLS certificate that ensure its identity to the client. It also contains the public key of the server.

**Step 4: Client Certificate (Client → Server, Optional)**

In rare cases, the server may require the client to be authenticated with a client certificate. If so, the client provides its signed certificate to the server.

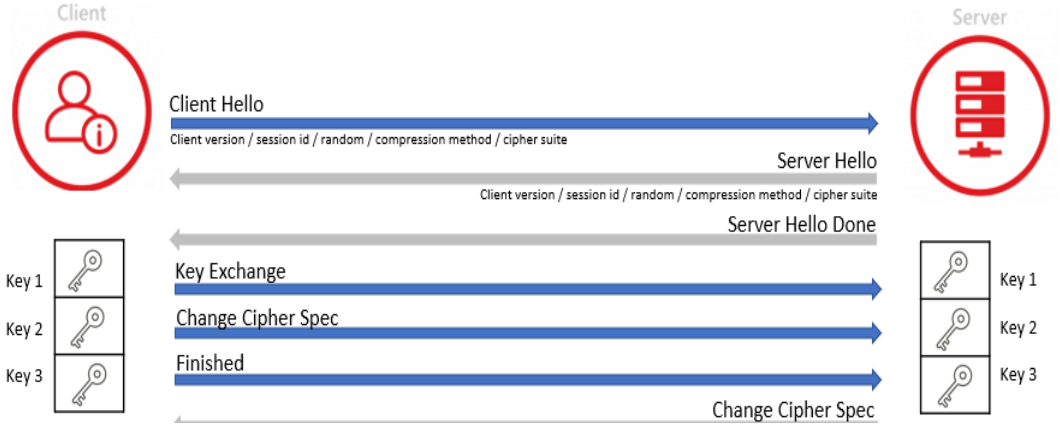
**Step 5: Server Key Exchange (Server → Client)**

The server key exchange message is sent only if the certificate provided by the server is not sufficient for the client to exchange the keys.

**Step 6: Server Hello Done (Server → Client)**

The server sends this to the client to confirm that the Server Hello message is finished.

**Step 7: Client Key Exchange (Server → Client)**



The Client Key Exchange message is sent right after the Server Hello Done is received from the server. If the server requests a Client Certificate, the Client Key Exchange is sent after that. During this stage, the client creates a pre-master key.

**Step 8: Client Change Cipher Spec (Client → Server)**

At this point, the client is ready to switch to a secure, encrypted environment. The Change Cipher Spec protocol is used to change the encryption. Any data sent by the client from now on will be encrypted using the symmetric shared key.

**Step 9: Client Handshake Finished (Client → Server)**

The last message of the handshake process from the client signifies that the handshake is finished. This is also the first encrypted message of the secure connection.

**Step 10: Server Change Cipher Spec (Server → Client)**

The server is also ready to switch to an encrypted environment. Any data sent by the server from now on will be encrypted using the symmetric shared key.

**Step 11: Server Handshake Finished (Server → Client)**

The last message of the handshake

## 2. CONCLUSION

As technology growths, vulnerabilities are discovered and new attacks are developed. for now and the foreseeable future, it looks like TLS will still be one of the main and most reliable tools that we use to secure our online world and Using multiple key instead of single key will enhance the security of TLS.

## REFERENCES

[1] https://patents.google.com/patent/CN102510387B/en?q=TLS+Handshake&oq=TLS+Handshake

[2] https://patents.google.com/patent/US20180091483A1/en?q=TLS+encryption&oq=TLS+encryption