Channel Encryption

A channel encryption is a process of restricting the overhearing and tampering in data communication. Most of the common channel encryption are HTTPS and TLS.

* Transmission Layer Security 1.2: The TLS is the most widely used protocol for implementing cryptography in web. A TLS provides secure communication channel to traditional TCP/IP protocol suite.

Table: TCP/IP Protocol stack with TLS

|  |  |
| --- | --- |
| **TCP/IP Layer** | **Protocol** |
| Internet layer | IP |
| Transmission Control Protocol | TCP |
| Transport Security Layer | TLS |
| Application Layer | NNTP, HTTP, FTP & Telnet |

TLS uses public-key cryptography to provide authentication, and secret-key cryptography with hash functions to provide for privacy and data integrity.

The reason behind the TLS use is that various cryptographic algorithms are being involving in the protocol. TLS uses secret-key and public-key cryptography to provide privacy and data integrity and, authentication respectively.

**SECRET KEY ALGORITHM**

In secret key algorithm, sender and receiver should have same secret key to perform encryption and decryption. Before start sending message over a secure communication channel, secret key must be available at the both parties to do encryption and decryption. The below section depicts sample encryption and decryption algorithms.

1. **Encryption algorithm**
2. Obtain an ASCII values of the plain text
3. Generate binary for given text.
4. Calculate 1’s complement and reverse the number
5. Take any four digits as a key e.g., 1011 and then divide the reserved number with chosen key
6. Obtain and store quotient and remainder in first 5 and last 3 digits. If those are less than 5 and 3 digits, then add sufficient number of 0’s. The result would be the cipher text.
7. **Decryption algorithm**
8. Obtain first 5 digits and multiply with key and add last 3 digits cipher to result
9. Reverse the output and then get the 1’s complement of it.
10. Identify the decimal equivalent to get the actual ASCII, which is plain text.

As the above algorithm uses same key for both encryption and decryption, it is called as symmetric algorithm. Well-known cryptographic algorithms are Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4) and Triple Data Encryption Standard (3DES).

[Experian Algorithm](http://www.experian.com/)

**Public-Key Cryptography**

Public-key cryptography solves the logistical problem of key distribution by using both a public key and a private key. The public key can be sent openly through the network while the private key is kept private by one of the communicating parties. The public and the private keys are cryptographic inverses of each other; what one key encrypts, the other key will decrypt.