Cybersecurity & Encryption Overview Cheat Sheet

by DaveLee via cheatography.com/186743/cs/39042/

Symmetric encryption algorithms

When encrypting and decrypting data, symmetric encryption algorithms employ the same secret key.

DES (Data Encryption Standard) is a block cipher that works with 64-bit data blocks and a 56-bit key. Due to its short key size, it is no longer regarded as secure for the majority of applications.

3DES (Triple Data Encryption Standard) is a block cipher that employs two or three separate keys to apply DES three times to each block of data. Although slower, it offers more protection than DES.

AES (Advanced Encryption Standard) is a block cipher that works with data blocks of 128 bits and has key sizes that can range from 128, 192, or 256 bits. It is regarded as secure and is now the most extensively used symmetric encryption algorithm.

Blowfish: A block cipher that uses 64-bit data blocks and keys up to 448 bits in size. Although it is quick and has a long history of use, it is no longer regarded as secure for several purposes.

Block cipher that uses a 128-bit key and 64-bit data blocks is called IDEA (International Data Encryption Algorithm). Its small block size means that it is no longer extensively utilized.

RC2 (Rivest Cipher 2) is a block cipher that works with data blocks that are 64 bits in size and uses keys up to 128 bits in size. Despite being frequently used in the past, it is today viewed as insecure.

RC4 (Rivest Cipher 4) is a stream cipher that supports keys up to 2048 bits in length. Although it was popular and quick, it is now viewed as being unsafe.

Symmetric encryption algorithms (cont)

RC5 (Rivest Cipher 5) is a block cipher that works with variable-length data blocks and keys up to 2048 bits in size. It is rarely employed.

RC6 (Rivest Cipher 6) is a block cipher that works with variable-length data blocks and keys up to 2048 bits in size. It is rarely employed.

A block cipher that uses 64-bit data blocks and keys up to 128 bits in size is called **CAST** (Carlisle Adams and Stafford Tavares). It is rarely employed.

MARS (Multiple-Algorithm Rijndael Substitution) is a block cipher that works with data blocks that are 128 bits in size and has a 128-bit key. For usage in high-security settings, IBM created it.

Serpent: A block cipher that uses 128-bit data blocks and keys up to 256 bits in size. Although it is slower than other algorithms, it is regarded as secure.

Twofish: A block cipher that works with data blocks of 128 bits and has key sizes up to 256 bits. Although it is slower than other algorithms, it is regarded as secure.

As a network authentication protocol, **Kerberos** uses encryption to safeguard authentication messages. It is not an encryption method.

SSL Cipher: The Secure Sockets Layer (SSL) protocol offers secure internet communication. AES, RC4, and 3DES are just a few of the encryption algorithms it uses. The SSL connection's setup determines the particular cipher that is employed.

What is Symmetric Cryptography?

Spoofing attack

IP spoofing	a technique used by attackers to disguise their true identity and location by sending data packets to a target system from a spoofed (fake) source IP address.
Email spoofing:	when an attacker sends an email with a fake "From" address to make the receiver believe it is coming from a reliable source. This can be used to launch phishing attacks, distribute malware, or steal confidential data.
DNS spoofing:	When a hacker modifies DNS (Domain Name System) records, traffic is redirected to a false website or a malicious IP address.
Caller ID Spoofing:	An attacker can pose as a legitimate caller and deceive the recipient into giving up personal information or sending money by using a spoof caller ID.
MAC Address Spoofing:	An attacker modifies their device's Media Access Control (MAC) address to pretend to be another device on the network and obtain access to resources that are restricted.

By **DaveLee**
cheatography.com/davelee/

Published 31st May, 2023.
Last updated 31st May, 2023.

Cybersecurity & Encryption Overview Cheat Sheet

by DaveLee via cheatography.com/186743/cs/39042/

Man in the middle attack

WiFi hijacking:	Hardware tool that hackers employ to launch man-in-the-middle assaults on wireless networks, called a pineapple.
SSL Stripping:	a type of man-in-the-middle attack that converts HTTPS--encrypted communication to HTTP, enabling the attacker to intercept or alter the communication.
Banking Trojans:	Malware that eavesdrops on users' communications with their banks in order to obtain login information and carry out fraudulent transactions.
Email hijacking:	A cyberattack in which the perpetrator intercepts emails transmitted between two parties and changes their contents. Scams involving corporate email compromise (BEC) frequently employ this approach.

SSL

The SSL protocol is composed of two parts:

the SSL Handshake Protocol, which creates the secure channel and verifies the server's identity.

The SSL Application Data Protocol is used to exchange data over a secure channel using encryption with a shared secret key established during the handshake.

Steps of handshake protocol:

SSL (cont)

The client uses the supported encryption techniques and the SSL version to send a greeting to the server.

The chosen SSL version and encryption algorithm are sent in the server's hello message.

To verify its identity, the server delivers its digital certificate.

After confirming the server's digital certificate, the client sends a message to say the handshake has been successful.

All subsequent communication between the client and server is encrypted using the shared secret key and the encryption technique that was previously agreed upon.

SSL FAQ: https://www.ssl.com/faqs/faq-what-is-ssl/

Asymmetric encryption (non-repudiation)

Asymmetric encryption, commonly referred to as ""public-key encryption,", uses two mathematically related keys: a public key for data encryption and a private key for data decryption. While the private key needs to be kept a secret, the public key can be shared with anybody.

RSA is a commonly used algorithm for secure data transfer, digital signatures, and data at rest encryption. It is named after its three creators, Rivest, Shamir, and Adleman.

Diffie-Hellman: A method for securely exchanging keys between two parties without requiring that they first divulge a secret key.

Elliptic Curve Cryptography (ECC): A more recent encryption technique that generates keys, performs encryption and decryption, and uses elliptic curves as the key generation mechanism.

Asymmetric encryption (non-repudiation) (cont)

With the help of the **DSA (Digital Signature Algorithm)**, it is possible to create digital signatures that can be verified without disclosing the secret key.

ElGamal: A public-key cryptographic system that is suitable for both digital signatures and encryption.

PGP (Pretty Good Privacy) is an encryption tool that offers secure data storage and communication by combining symmetric and asymmetric encryption methods.

Asymmetric Key Encryption Explained

Authentication

Username and Password	To access a system, application, or network, users must input a special username and password.
Two-Factor Authentication	Users must enter two distinct forms of identification to gain access, such as a password and a special code created by an authentication app or texted to them.

Authentication (cont)

Biometric authentication	is frequently employed in mobile devices and other systems, uses distinctive physical traits like fingerprints or face recognition to confirm a user's identification.
Smart Card Authentication	To confirm the user's identification, a physical card with a microprocessor chip is put into a reader.
Certificate-based Authentication	Digital certificates, which contain information like public keys or digital signatures, are issued by a trusted authority and are used to confirm the identification of people or devices.
Token--Based Authentication	A token, such as a USB key or smart card, is used to hold authentication credentials that can be used to confirm a user's identity.

Authentication (cont)

Kerberos Authentication	Kerberos is a network authentication protocol that employs tickets to authenticate users and provide them access to network resources.
OAuth	OAuth is an open standard for authentication that enables users to authorize access to their accounts or data without disclosing their username and password.
XML-based SAML authentication	a standard for transferring authentication and authorization information between parties. SAML stands for Security Assertion Markup Language.
Remote Authentication Dial-In User Service (RADIUS)	a networking protocol that offers centralized authentication, authorization, and accounting for network access.

Remote access

Local area networks (LANs) employ the 802.11 wireless networking standard.

A **virtual private network**, or VPN, establishes a safe, encrypted connection over the internet to enable network access from a distance.

Dial-Up Network A technique called networking is used to link a computer to the internet over a phone connection.

Remote Access ID and User Service A networking protocol called **Dial-In User Service** offers centralized network access authentication, authorization, and accounting.

TACACS: Terminal Access Controller Access Control System is a protocol used in networked computing systems for remote authentication and authorization.

TACACS+: An improved version of TACACS with more security features.

Secure Sockets Layer, or SSL, is a protocol that enables secure internet communication.

To guarantee secure communication across IP networks, a protocol suite called **IPSec**—Internet Protocol Security—is utilized.

A protocol called **Remote Desktop Protocol (RDP)** is used to grant remote access to a Windows-running machine or server.

Trojans that allow an attacker to enter a victim's computer or network without authorization are known as remote access trojans (RATs).

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables users to connect remotely via the internet to a network.

Cybersecurity & Encryption Overview Cheat Sheet

by DaveLee via cheatography.com/186743/cs/39042/

Remote access (cont)

SSH is a network protocol that enables secure remote access to a server or computer over an unsafe network.

Access control

MAC	A central authority-controlled set of predetermined rules govern access. It is frequently employed in official and military settings.
DAC	Access is controlled by the resource owner; commonly used in homes and small companies.
RBAC	Access is determined by the user's role, and it's frequently employed in big businesses.

Key management and certificate life cycle

Key Generation:	The entity requesting a digital certificate generates a public key pair.
Identity Submission:	The entity informs a Certificate Authority (CA) of its identity.
Registration	The CA registers the request after verifying the identity details.
Certification	Using its own private key, the CA generates a digital certificate including the entity's public key and other identifying information

Key management and certificate life cycle (cont)

Distribution	The CA gives the certificate to the organization or makes it accessible to the general public.
Usage:	The entity may establish secure communications with other entities and self-authenticate using the certificate.
Expiration:	The certificate may expire or be revoked if it has been compromised. It also has a time limit.
Renewal:	A fresh key pair and certificate may be created as needed.
Recovery:	In the event that a private key is misplaced or stolen, a recovery procedure can be started to reclaim access to the certificate.
Archive:	For future reference and auditing needs, certificates and the keys that go with them are securely kept.
HSM:	A physical device that strengthens encryption by generating keys, creating and verifying digital signatures, and encrypting / decrypting data.

Key Management in the Cloud

Key management vs PKI management

Key management	PKI management
the secure creation, distribution, archival, and deletion of cryptographic keys is a concern	concerned with the production, distribution, and maintenance of digital certificates and related keys
Messages are encrypted and decrypted using keys, which are also used to authenticate users and create secure connections.	Digital certificates are employed to confirm the parties to a transaction's identification and to guarantee the veracity and integrity of the data being communicated.
Key management is concerned with handling cryptographic keys safely.	Establishing trust and ensuring secure communication between parties is the main goal of PKI management.
makes sure that keys are correctly utilized and safeguarded from unauthorized access or abuse	involves revoking digital certificates that are either hacked or have lost their validity.

PKI explained

Kerberos

Kerberos is a network authentication protocol that offers safe client/server application authentication over insecure networks using symmetric key cryptography and a reliable third-party Key Distribution Center (KDC). Widely used in business networks, it is protected against replay attacks, eavesdropping, and man-in-the-middle attacks.

Cybersecurity & Encryption Overview Cheat Sheet

by DaveLee via cheatography.com/186743/cs/39042/

Hash

BLAKE2	A quick and secure hashing algorithm that generates hash values of various sizes.
RIPEMD	A group of hashing algorithms that includes RIPEMD-160, a 160-bit hash value generator.
Whirlpool	A powerful hash function that generates 512-bit hash values.
SHA	A group of cryptographic hashing algorithms created by the NSA. The most used (256-bit hash) is SHA-256. An older version, SHA-1, is currently insecure.
SHA-3	The most recent member of the SHA family, SHA-3, generates hash values of various sizes and is thought to be more secure than its forerunners.
Tiger	A hash function that generates 192-bit hash values and is renowned for its quickness and effectiveness.
MD	Ron Rivest's hash function family. A 128-bit hash value is generated by MD5, whereas 160-bit and 128-bit hash values are generated by MD2 and MD4, respectively.

DOS attack

Ping flood attack:	The attacker floods the victim's IP address with ping queries, overloading the victim's network and causing it to slow down or crash.

DOS attack (cont)

SYN flood attack:	The attacker floods the victim's server with SYN requests, exhausting its resources and making it crash or stop responding.
Smurf attack:	The victim's network may be overrun by a flood of responses as a result of the attacker sending numerous ICMP echo queries to IP broadcast addresses.
UDP flood attack:	The attacker floods the victim's network with UDP packets, eating up all of its resources and causing it to slow down or crash.
HTTP flood attack:	The attacker bombards a target website with numerous HTTP requests, utilizing up all of its resources and making it unresponsive.
DNS flood attacks:	The victim's DNS servers are crashed or rendered unavailable as a result of the attacker sending a lot of DNS requests to them.

DOS attack (cont)

Attacks using NTP Amplification:	The attacker takes advantage of weak NTP servers to increase the amount of traffic transmitted to the victim.
Attacks by Slowloris:	involve opening several connections to the victim's server and sending fragmented HTTP requests, which drain server resources and cause the server to become unusable.

By **DaveLee**
cheatography.com/davelee/

Published 31st May, 2023.
Last updated 31st May, 2023.