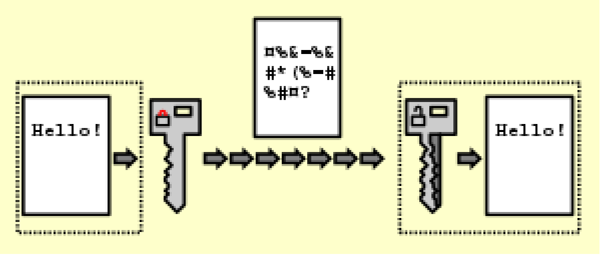
WIKIPEDIA
The Free Encyclopedia

Encryption

In cryptography, **encryption** is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.



A simple illustration of public-key cryptography, one of the most widely used forms of encryption

For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is possible to decrypt the message without possessing the key but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

Historically, various forms of encryption have been used to aid in cryptography. Early encryption techniques were often used in military messaging. Since then, new techniques have emerged and become commonplace in all areas of modern computing.[1] Modern encryption schemes use the concepts of public-key and symmetric-key.[1] Modern encryption techniques ensure security because modern computers are inefficient at cracking the encryption.

History

Ancient

One of the earliest forms of encryption is symbol replacement, which was first found in the tomb of Khnumhotep II, who lived in 1900 BC Egypt. Symbol replacement encryption is “non-standard,” which means that the symbols require a cipher or key to understand. This type of early encryption was used throughout Ancient Greece and Rome for military purposes.[2] One of the most famous military encryption developments was the Caesar Cipher, which was a system in which a letter in normal text is shifted down a fixed number of positions down the alphabet to get the encoded letter. A message encoded with this type of encryption could be decoded with the fixed number on the Caesar Cipher.[3]

Around 800 AD, Arab mathematician Al-Kindi developed the technique of frequency analysis – which was an attempt to systematically crack Caesar ciphers.[2] This technique looked at the frequency of letters in the encrypted message to determine the appropriate shift. This technique was rendered ineffective after the creation of the Polyalphabetic cipher by Leone Alberti in 1465, which incorporated different sets of languages. In order for frequency analysis to be useful, the person trying to decrypt the message would need to know which language the sender chose.[2]

19th–20th century

Around 1790, Thomas Jefferson theorized a cipher to encode and decode messages in order to provide a more secure way of military correspondence. The cipher, known today as the Wheel Cipher or the Jefferson Disk, although never actually built, was theorized as a spool that could jumble an English message up to 36 characters. The message could be decrypted by plugging in the jumbled message to a receiver with an identical cipher.[4]

A similar device to the Jefferson Disk, the M-94, was developed in 1917 independently by US Army Major Joseph Mauborne. This device was used in U.S. military communications until 1942.[5]

In World War II, the Axis powers used a more advanced version of the M-94 called the Enigma Machine. The Enigma Machine was more complex because unlike the Jefferson Wheel and the M-94, each day the jumble of letters switched to a completely new combination. Each day's combination was only known by the Axis, so many thought the only way to break the code would be to try over 17,000 combinations within 24 hours.[6] The Allies used computing power to severely limit the number of reasonable combinations they needed to check every day, leading to the breaking of the Enigma Machine.

Modern

Today, encryption is used in the transfer of communication over the Internet for security and commerce.[1] As computing power continues to increase, computer encryption is constantly evolving to prevent eavesdropping attacks.[7] With one of the first “modern” cipher suits, DES, utilizing a 56-bit key with 72,057,594,037,927,936 possibilities being able to be cracked in 22 hours and 15 minutes by EFF’s DES cracker in 1999, which used a brute-force method of cracking. Modern encryption standards often use stronger key sizes often 256, like AES(256-bit mode), TwoFish, ChaCha20-Poly1305, Serpent(configurable up to 512-bit). Cipher suits utilizing a 128-bit or higher key, like AES, will not be able to be brute-forced due to the total amount of keys of 3.4028237e+38 possibilities. The most likely option for cracking ciphers with high key size is to find vulnerabilities in the cipher itself, like inherent biases and backdoors. For example, RC4, a stream cipher was cracked due to inherit biases and vulnerabilities in the cipher.

Encryption in cryptography

In the context of cryptography, encryption serves as a mechanism to ensure confidentiality.[1] Since data may be visible on the Internet, sensitive information such as passwords and personal communication may be exposed to potential interceptors.[1] The process of encrypting and decrypting messages involves keys. The two main types of keys in cryptographic systems are symmetric-key and public-key (also known as asymmetric-key).[8][9]

Many complex cryptographic algorithms often use simple modular arithmetic in their implementations.[10]

Types

In symmetric-key schemes,[11] the encryption and decryption keys are the same. Communicating parties must have the same key in order to achieve secure communication. The German Enigma Machine utilized a new symmetric-key each day for encoding and decoding messages.

In public-key encryption schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key that enables messages to be read.[12] Public-key encryption was first described in a secret document in 1973;[13] beforehand, all encryption schemes were symmetric-key (also called private-key).[14]:478 Although published subsequently, the work of Diffie and Hellman was published in a journal with a large readership, and the value of the methodology was explicitly described.[15] The method became known as the Diffie-Hellman key exchange.

RSA (Rivest–Shamir–Adleman) is another notable public-key cryptosystem. Created in 1978, it is still used today for applications involving digital signatures.[16] Using number theory, the RSA algorithm selects two prime numbers, which help generate both the encryption and decryption keys.[17]

A publicly available public-key encryption application called Pretty Good Privacy (PGP) was written in 1991 by Phil Zimmermann, and distributed free of charge with source code. PGP was purchased by Symantec in 2010 and is regularly updated.[18]

Uses

Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage.[19] Encryption can be used to protect data "at rest", such as information stored on computers and storage devices (e.g. USB flash drives). In recent years, there have been numerous reports of confidential data, such as customers' personal records, being exposed through loss or theft of laptops or backup drives; encrypting such files at rest helps protect them if physical security measures fail.[20][21][22] Digital rights management systems, which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering (see also copy protection), is another somewhat different example of using encryption on data at rest.[23]

Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years.[24] Data should also be encrypted when transmitted across networks in order to protect against eavesdropping of network traffic by unauthorized users.[25]

Data erasure

Conventional methods for permanently deleting data from a storage device involve overwriting the device's whole content with zeros, ones, or other patterns – a process which can take a significant amount of time, depending on the capacity and the type of storage medium. Cryptography offers a way of making the erasure almost instantaneous. This method is called crypto-shredding. An example implementation of this method can be found on iOS devices, where the cryptographic key is kept in a dedicated 'effaceable storage'.[26] Because the key is stored on the same device, this setup on its own does not offer full privacy or security protection if an unauthorized person gains physical access to the device.

Limitations

Encryption is used in the 21st century to protect digital data and information systems. As computing power increased over the years, encryption technology has only become more advanced and secure. However, this advancement in technology has also exposed a potential limitation of today's encryption methods.

The length of the encryption key is an indicator of the strength of the encryption method.[27] For example, the original encryption key, DES (Data Encryption Standard), was 56 bits, meaning it had 2^56 combination possibilities. With today's computing power, a 56-bit key is no longer secure, being vulnerable to hacking by brute force attack.[28]

Quantum computing utilizes properties of quantum mechanics in order to process large amounts of data simultaneously. Quantum computing has been found to achieve computing speeds thousands of times faster than today's supercomputers.[29] This computing power presents a challenge to today's encryption technology. For example, RSA encryption utilizes the multiplication of very large prime numbers to create a semiprime number for its public key. Decoding this key without its private key requires this semiprime number to be factored in, which can take a very long time to do with modern computers. It would take a supercomputer anywhere between weeks to months to factor in this key. However, quantum computing can use quantum algorithms to factor this semiprime number in the same amount of time it takes for normal computers to generate it. This would make all data protected by current public-key encryption vulnerable to quantum computing attacks.[30] Other encryption techniques like elliptic curve cryptography and symmetric key encryption are also vulnerable to quantum computing.

While quantum computing could be a threat to encryption security in the future, quantum computing as it currently stands is still very limited. Quantum computing currently is not commercially available, cannot handle large amounts of code, and only exists as computational devices, not computers.[31] Furthermore, quantum computing advancements will be able to be utilized in favor of encryption as well. The National Security Agency (NSA) is currently preparing post-quantum encryption standards for the future.[32] Quantum encryption promises a level of security that will be able to counter the threat of quantum computing.[31]

Attacks and countermeasures

Encryption is an important tool but is not sufficient alone to ensure the security or privacy of sensitive information throughout its lifetime. Most applications of encryption protect information only at rest or in transit, leaving sensitive data in clear text and potentially vulnerable to improper disclosure during processing, such as by a cloud service for example. Homomorphic encryption and secure multi-party computation are emerging techniques to compute on encrypted data; these techniques are general and Turing complete but incur high computational and/or communication costs.

In response to encryption of data at rest, cyber-adversaries have developed new types of attacks. These more recent threats to encryption of data at rest include cryptographic attacks,[33] stolen ciphertext attacks,[34] attacks on encryption keys,[35] insider attacks, data corruption or integrity attacks,[36] data destruction attacks, and ransomware attacks. Data fragmentation[37] and active defense[38] data protection technologies attempt to counter some of these attacks, by distributing, moving, or mutating ciphertext so it is more difficult to identify, steal, corrupt, or destroy.[39]

The debate around encryption

The question of balancing the need for national security with the right to privacy has been debated for years, since encryption has become critical in today's digital society. The modern encryption debate[40] started around the '90 when US government tried to ban cryptography because, according to them, it would threaten national security. The debate is polarized around two opposing views. Those who see strong encryption as a problem making it easier for criminals to hide their illegal acts online and others who argue that encryption keep digital communications safe. The debate heated up in 2014, when Big Tech like Apple and Google set encryption by default in their devices. This was the start of a series of controversies that puts governments, companies and internet users at stake.

Integrity protection of ciphertexts

Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message; for example, verification of a message authentication code (MAC) or a digital signature usually done by a hashing algorithm or a PGP signature. Authenticated encryption algorithms are designed to provide both encryption and integrity protection together. Standards for cryptographic software and hardware to perform encryption are widely available, but successfully using encryption to ensure security may be a challenging problem. A single error in system design or execution can allow successful attacks. Sometimes an adversary can obtain unencrypted information without directly undoing the encryption. See for example traffic analysis, TEMPEST, or Trojan horse.[41]

Integrity protection mechanisms such as MACs and digital signatures must be applied to the ciphertext when it is first created, typically on the same device used to compose the message, to protect a message end-to-end along its full transmission path; otherwise, any node between the sender and the encryption agent could potentially tamper with it. Encrypting at the time of creation is only secure if the encryption device itself has correct keys and has not been tampered with. If an endpoint device has been configured to trust a root certificate that an attacker controls, for example, then the attacker can both inspect and tamper with encrypted data by performing a man-in-the-middle attack anywhere along the message's path. The common practice of TLS interception by network operators represents a controlled and institutionally sanctioned form of such an attack, but countries have also attempted to employ such attacks as a form of control and censorship.[42]

Ciphertext length and padding

Even when encryption correctly hides a message's content and it cannot be tampered with at rest or in transit, a message's *length* is a form of metadata that can still leak sensitive information about the message. For example, the well-known CRIME and BREACH attacks against HTTPS were side-channel attacks that relied on information leakage via the length of encrypted content.[43] Traffic analysis is a broad class of techniques that often employs message lengths to infer sensitive implementation about traffic flows by aggregating information about a large number of messages.

Padding a message's payload before encrypting it can help obscure the cleartext's true length, at the cost of increasing the ciphertext's size and introducing or increasing bandwidth overhead. Messages may be padded randomly or deterministically, with each approach having different tradeoffs. Encrypting and padding messages to form padded uniform random blobs or PURBs is a practice guaranteeing that the cipher text leaks no metadata about its cleartext's content, and leaks asymptotically minimal $O(\log\log M)$ information via its length.[44]

See also

- Cryptosystem
- Cold boot attack
- Cyberspace Electronic Security Act (US)
- Dictionary attack
- Disk encryption
- Encrypted function
- Export of cryptography
- Geo-blocking
- Indistinguishability obfuscation
- Key management