Understanding Cryptography

Security level For example, AES-128 (key size 128 bits) is designed to offer a 128-bit security level, which is considered roughly equivalent to a RSA using 3072-bit key. Security level In cryptography, security level is a measure of the strength that a cryptographic primitive — such as a cipher or hash function — achieves. This allows for convenient comparison between algorithms and is useful when combining multiple primitives in a hybrid cryptosystem, so there is no clear weakest link. In cryptography, security level is a measure of the strength that a cryptographic primitive — such as a cipher or hash function — achieves. Security level is usually expressed as a number of "bits of security" (also security strength), where n-bit security means that the attacker would have to perform 2n operations to break it, but other methods have been proposed that more closely model the costs for an attacker 613378f212

Elliptic-curve cryptography ECC Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys to provide equivalent security, compared to cryptosystems based on modular exponentiation in finite fields, such as the RSA cryptosystem and ElGamal cryptosystem 613378f212

Before... 613378f212 The earliest known book on cryptography was an ancient work, now lost, but referred to by the ancient roman grammarian Aulus Gellius. He mentioned that an earlier grammarian named Probus wrote a book on the subject and that the book mentioned Julius Caesar's use of rudimentary cryptograms during his rule. The next work that we know of was Steganographia, sive Ars concealendi -- three volumes written by Johannes Trithemius. Though the books were about cryptography, he concealed this in mystical language which the Catholic Church mistook for black magic. It banned the work, listing it in the Index Librorum Prohibitorum. Many writers claimed to have invented unbreakable ciphers. None were, though it sometimes took a long while to establish this. 613378f212 In this context, security claim or target security level is the security level that a primitive was initially designed to achieve, although "security level" is also sometimes used in those contexts. When attacks are found that have lower cost than the security claim, the primitive is considered broken. 613378f212 Symmetric algorithms usually have a strictly defined security claim. For symmetric ciphers, it is typically equal to the key... 613378f212 The development of cryptography has been paralleled by the development of cryptanalysis — the "breaking" of codes and ciphers. The discovery and application, early on, of frequency analysis to the reading of encrypted communications has, on occasion, altered the course of history. Thus the Zimmermann Telegram triggered the United States' entry into World War I; and Allies reading of Nazi Germany's ciphers shortened World War II, in some evaluations by as much as two years. 613378f212 a data encapsulation scheme, which is a symmetric-key cryptosystem 613378f212

History of cryptography Until recent decades, it has been the story of what might be called classical Cryptography, the use of codes and ciphers, began thousands of years ago. Until recent decades, it has been the story of what might be called classical cryptography — that is, of methods of encryption that use pen and paper, or perhaps simple mechanical aids. Cryptography, the use of codes and ciphers, began thousands of years ago. In the early 20th century, the invention of complex mechanical and electromechanical machines, such as the Enigma rotor machine, provided more sophisticated and efficient means of encryption; and the subsequent introduction of electronics and computing has allowed elaborate schemes of still greater complexity, most of which are entirely unsuited to pen and paper 613378f212

n 613378f212 The hybrid cryptosystem is itself a public-key system, whose public and private keys are the same as in the key encapsulation scheme. 613378f212 == Early history == 613378f212

Bibliography of cryptography This is despite the paradox that secrecy is of the essence Books on cryptography have been published sporadically and with variable quality for a long time. This is despite the paradox that secrecy is of the essence in sending confidential messages – see Kerckhoffs' principle. Books on cryptography have been published sporadically and with variable quality for a long time 613378f212

Symmetric-key algorithm The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. The keys may be identical, or there may be a simple transformation to go between the two keys. The requirement that both parties have access to the secret key is one of the main drawbacks of symmetric-key encryption, in comparison to asymmetric-key encryption (also known as public-key encryption). With the exception of the one-time pad they have a smaller key size, which means less storage space and faster transmission. Due to this, asymmetric-key encryption is often used to exchange the secret key for symmetric-key encryption. However, symmetric-key encryption algorithms are usually better for bulk encryption. Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both the encryption of plaintext and the decryption of Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both the encryption of plaintext and the decryption of ciphertext 613378f212

== History == 613378f212 Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. They are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic-curve factorization. 613378f212 == In symmetric cryptography == 613378f212 Symmetric-key encryption can use either stream ciphers or block ciphers. 613378f212 == Types == 613378f212 == Description == 613378f212 In the 19th century, the general standard improved somewhat (e.g., works by Auguste... 613378f212 A hybrid cryptosystem can be constructed using any two separate cryptosystems: 613378f212

Hybrid cryptosystem Public-key cryptosystems are convenient in that they do not require the sender and receiver to share a common secret in order to communicate securely. "Chapter 6: Introduction to Public-Key Cryptography". This is addressed by hybrid systems by using a combination of both. In many applications, the high cost of encrypting long messages in a public-key cryptosystem can be prohibitive. Springer In cryptography, a hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. Understanding Cryptography: A Textbook for Students and Practitioners (PDF). Bart (2010). However, they often rely on complicated mathematical computations and are thus generally much more inefficient than comparable symmetric-key cryptosystems 613378f212

Cryptography law There are many different Cryptography is the practice and study of encrypting information, or in other words, securing information from unauthorized access. There are many different cryptography laws in different nations. Some countries require decryption keys to be recoverable in case of a police investigation. Some countries prohibit the export of cryptography software and/or encryption algorithms or cryptoanalysis methods. Cryptography is the practice and study of encrypting information, or in other words, securing information from unauthorized access 613378f212

In contrast, the revolutions in cryptography and secure communications since the 1970s are covered in the available literature. 613378f212 Until the 1960s, secure cryptography was largely the preserve of governments. Two events have since... 613378f212 Public key algorithms are fundamental security primitives in modern cryptosystems, including applications and protocols that offer assurance of the confidentiality and authenticity of electronic communications and data storage. They underpin numerous Internet standards, such as Transport Layer Security (TLS), SSH, S/MIME, and PGP. Compared to symmetric cryptography, public-key cryptography can be too slow for many purposes, so these protocols often combine symmetric cryptography with public-key cryptography in hybrid cryptosystems. 613378f212 a key encapsulation mechanism, which is a public-key cryptosystem 613378f212 == Overview == 613378f212

Cryptography More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages. Core concepts related to information security (data confidentiality, data integrity, authentication and non-repudiation) are also central to cryptography. Cryptography, or cryptology, is the practice and study of techniques for secure communication in the presence of adversarial behavior. Practical applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords and military communications. More generally, Cryptography, or cryptology, is the practice and study of techniques for secure communication in the presence of adversarial behavior. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, information security, electrical engineering, digital signal processing, physics, and others 613378f212

Cryptographic hash function A cryptographic hash function (CHF) is a hash algorithm (a map of an arbitrary binary string to a binary string with a fixed size of n {\displaystyle A cryptographic hash function (CHF) is a hash algorithm (a map of an arbitrary binary string to a binary string with a fixed size of 613378f212

Issues regarding cryptography law fall into four categories: 613378f212 Stream ciphers encrypt the digits (typically bytes), or letters (in substitution ciphers) of a message one at a time. An example is ChaCha20. Substitution ciphers are well-known ciphers, but can be... 613378f212 Cryptography prior to the modern age was effectively synonymous with encryption, converting readable information (plaintext) to unintelligible nonsense text (ciphertext), which can only be read by reversing the process (decryption). The sender of an encrypted (coded) message shares the decryption (decoding) technique only with the intended recipients to preclude access from adversaries. The cryptography literature... 613378f212

Public-key cryptography Key pairs are generated with algorithms based on mathematical problems termed one-way functions. Each key pair consists of a public key and a corresponding private key. There are many kinds of public-key cryptosystems, with different security goals, including digital signature, Diffie–Hellman key exchange, public-key key encapsulation, and public-key encryption. Each key pair consists of a Public-key cryptography, or asymmetric cryptography, is the field of cryptographic systems that use pairs of related keys. Security of public-key cryptography depends on keeping the private key secret; the public key can be openly distributed without compromising security. Public-key cryptography, or asymmetric cryptography, is the field of cryptographic systems that use pairs of related keys 613378f212

Note that for very long messages the bulk of the work in encryption/decryption is done by the more efficient symmetric-key scheme, while the inefficient public-key scheme is used only to encrypt/decrypt a short... 613378f212