Difference Between Cryptography And Steganography

== Example == 10a41bca8b

Steganography For example, the hidden message may be in invisible ink between the visible lines of a private letter. In computing and electronic contexts, a computer file, message, image, or video is concealed within another file, message, image, or video. Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Some implementations of steganography that lack a formal shared secret are forms of security through obscurity, while key-dependent steganographic schemes try to adhere to Kerckhoffs's principle. The advantage of steganography over cryptography alone is that the intended Steganography (STEG-ə-NOG-rə-fee) is the practice of representing information within another message or physical object, in such a manner that the presence of the concealed information would not be evident to an unsuspecting person's examination. Generally, the hidden messages appear to be (or to be part of) something else: images, articles, shopping lists, or some other cover text 10a41bca8b

The X.509 public key certificate illustrates crypto-agility. A public key certificate has cryptographic parameters including key type, key length, and a hash algorithm. X.509 version v.3, with key type RSA, a 1024-bit key length, and the SHA-1 hash algorithm were found by... 10a41bca8b Artificial neural networks are well known for their ability to selectively explore the solution space of a given problem. This feature finds a natural niche of application in the field of cryptanalysis. At the same time, neural networks offer a new approach to attack ciphering algorithms based on the principle that any function could be reproduced by a neural network, which is a powerful proven computational tool that can be used to find the inverse-function of any cryptographic algorithm. 10a41bca8b

Quantum cryptography Quantum cryptography is the exploiting of quantum-mechanical properties such as quantum entanglement, measurement disturbance, no-cloning theorem, and the Quantum cryptography is the exploiting of quantum-mechanical properties such as quantum entanglement, measurement disturbance, no-cloning theorem, and the principle of superposition to perform encryption tasks. Quantum encryption plays a crucial role in the secure processing, storage, and transmission of information 10a41bca8b

Johannes Trithemius His students included Heinrich Cornelius Agrippa and Paracelsus. He had considerable influence on the development of early modern and modern occultism. He is considered the founder of modern cryptography (a claim shared with Leon Battista Alberti) and steganography, as well as the founder of bibliography and literary studies as branches of knowledge. founder of modern cryptography (a claim shared with Leon Battista Alberti) and steganography, as well as the founder of bibliography and literary studies Johannes Trithemius (; 1 February 1462 – 13 December 1516), born Johann Heidenberg, was a German Benedictine abbot and a polymath who was active in the German Renaissance as a lexicographer, chronicler, cryptographer, and occultist 10a41bca8b

The ideas of mutual learning, self learning, and stochastic behavior of neural networks and similar algorithms can be used for different aspects of cryptography, like public-key cryptography, solving the key distribution problem using neural network mutual synchronization, hashing or generation of pseudo-random numbers. 10a41bca8b

S-box In cryptography, an S-box (substitution-box) is a basic component of symmetric key algorithms which performs substitution. Mathematically, an S-box is a nonlinear vectorial Boolean function. In block ciphers, they are typically In cryptography, an S-box (substitution-box) is a basic component of symmetric key algorithms which performs substitution. In block ciphers, they are typically used to obscure the relationship between the key and the ciphertext, thus ensuring Shannon's property of confusion 10a41bca8b

Until the 1960s, secure cryptography was largely the preserve of governments. Two events have since... 10a41bca8b When Johannes was still an infant his father, Johann von Heidenburg, died. His stepfather, whom his mother Elisabeth married seven years later, was hostile to education and thus Johannes could only learn in secret and with many difficulties. He learned Greek, Latin, and Hebrew. When he was 17 years old he escaped from his home and wandered around looking for good teachers, travelling to Trier, Cologne, the Netherlands, and Heidelberg. He studied at the University... 10a41bca8b

Key (cryptography) Based on the used method, the key can be different sizes and varieties, but A key in cryptography is a piece of information, usually a string of numbers or letters that are stored in a file, which, when processed through a cryptographic algorithm, can encode or decode cryptographic data. A key's security strength is dependent on its algorithm, the size of the key, the generation of the key, and the process of key exchange. processed through a cryptographic algorithm, can encode or decode cryptographic data. Based on the used method, the key can be different sizes and varieties, but in all cases, the strength of the encryption relies on the security of the key being maintained 10a41bca8b

One good example of a fixed table is the S-box from DES (S5), mapping 6-bit input into a 4-bit output: 10a41bca8b

Cryptographic agility A cryptographically In cryptographic protocol design, cryptographic agility or crypto-agility is the ability to switch between multiple cryptographic primitives. In cryptographic protocol design, cryptographic agility or crypto-agility is the ability to switch between multiple cryptographic primitives 10a41bca8b

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 10a41bca8b

== Example == 10a41bca8b In general, an S-box takes some number of input bits, m, and transforms them into some number of output bits, n, where n is not necessarily equal to m. An m×n S-box can be implemented as a lookup table with 2m words of n bits each. Fixed tables are normally used, as in the Data Encryption Standard (DES), but in some ciphers the tables are generated dynamically from the key (e.g. the Blowfish and the Twofish encryption algorithms). 10a41bca8b

Salt (cryptography) Additionally, salting does not place any burden on users. rainbow tables), by vastly growing the size of table needed for a successful attack. g. It also helps protect passwords that occur multiple times in a database, as a new salt is used for each password instance. Salting helps defend against attacks that use precomputed tables (e. Salting helps defend In cryptography, a salt is random data fed as an additional input to a one-way function that hashes data, a password or passphrase. In cryptography, a salt is random data fed as an additional input to a one-way function that hashes data, a password or passphrase 10a41bca8b

Another idea is the ability of a neural network to separate space in non-linear pieces using "bias". It gives different probabilities of activating the neural network... 10a41bca8b Typically, a unique salt is randomly generated for each password. The salt and the password (or its version after key stretching) are concatenated and fed to a cryptographic hash function, and the output hash value is then stored with the salt in a database. The salt does not need to be encrypted, because knowing the salt would not help the attacker. 10a41bca8b These advantages make... 10a41bca8b The byname Trithemius refers to his native town of Trittenheim on the Moselle River, at the time part of the Electorate of Trier. 10a41bca8b Cryptographic agility acts as a safety measure or an incident response mechanism for when a cryptographic primitive of a system is discovered to be vulnerable. A security system is considered crypto-agile if its cryptographic algorithms or parameters can be replaced with ease and is at least partly automated. The impending arrival of a quantum computer that can break existing asymmetric cryptography is raising awareness of the importance of cryptographic agility. 10a41bca8b == Early life == 10a41bca8b The advantage of steganography... 10a41bca8b

Neural cryptography Neural cryptography is a branch of cryptography dedicated to analyzing the application of stochastic algorithms, especially artificial neural network algorithms Neural cryptography is a branch of cryptography dedicated to analyzing the application of stochastic algorithms, especially artificial neural network algorithms, for use in encryption and cryptanalysis 10a41bca8b

A cryptographically agile system implementing a particular standard can choose which combination of primitives to use. The primary goal of cryptographic agility is to enable rapid adaptations of new cryptographic primitives and algorithms without making disruptive changes to the system's infrastructure. 10a41bca8b == Example == 10a41bca8b n 10a41bca8b 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. 10a41bca8b The word steganography comes from Greek steganographia, which combines the words steganós (στεγανός), meaning "covered or concealed", and -graphia (γραφή) meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. 10a41bca8b == Scope == 10a41bca8b Without a salt, identical passwords will map to identical hash values, which could make it easier for a hacker to guess the passwords from their hash value. 10a41bca8b Furthermore, quantum cryptography affords the authentication of messages, which allows the legitimate parties to prove that the messages were not wiretapped during transmission. Thus, in a cryptographic set-up, it is impossible to copy, with perfect fidelity, the data encrypted in a quantum state. If one attempts to read the encrypted data, the quantum state will be changed due to wave function collapse (no-cloning theorem). This could be used to detect eavesdropping in QKD schemes, or in quantum communication links and networks. 10a41bca8b Salting is broadly used in cybersecurity, from Unix system credentials to Internet security. 10a41bca8b One aspect of quantum cryptography is quantum key distribution (QKD), which offers an information-theoretically secure solution to the key-exchange problem. Quantum cryptography allows the completion of cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e., non-quantum) communication. 10a41bca8b Salts are related to cryptographic nonces. 10a41bca8b The key is what is used to encrypt data from plaintext to ciphertext. There are different methods for utilizing keys and encryption. 10a41bca8b == Definition == 10a41bca8b

History of cryptography systems Steganography Timeline of cryptography Outline of cryptography World War I cryptography World War II cryptography "A Brief History of Cryptography". 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. 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 10a41bca8b

https://lb1-s245-pub.pressidium.com/~o/book/dl?EPUB=circuit-breaker-circuit-breaker