5 popular encryption algorithms you should know

You have heard or used encryption and know how important it is. Most Internet services use encryption to keep user information safe. However, coding is still something difficult to understand. There are many types of encryption and are used for many purposes. How do you know the 'best' encoding?

You have heard or used encryption and know how important it is. Most Internet services use encryption to keep user information safe. However, coding is still something difficult to understand. There are many types of encryption and are used for many purposes. How do you know the "best" encoding? Let's see how some of the following encryption types work, and why you should not create your own encryption.

Compare encryption type with encryption strength

Encryption terms such as encryption, encryption algorithms and encryption strength often confuse users, analyze it:

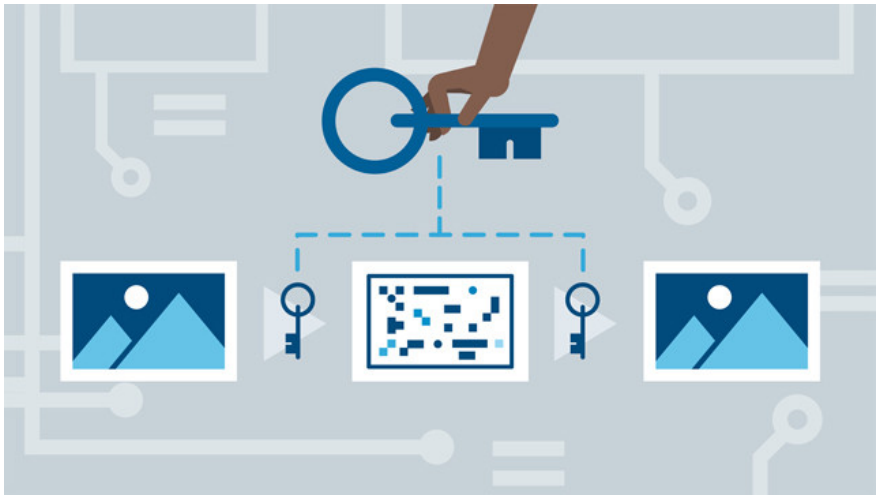
1. **Encryption type** : is the type of encryption related to how the encoding is completed. For example, symmetric encryption (asymmetric cryptography) is one of the most popular types of encryption on the Internet.
2. **Encryption algorithm** : When talking about encryption strength, we often talk about a specific encryption algorithm. Algorithms have interesting names like Triple DES, RSA or AES. Encryption algorithm names often come with numerical values, such as AES-128. This number refers to the size of the encryption key and further determines the strength of the algorithm.

5 most popular encryption algorithms

Encryption types form the basis of encryption algorithms, while encryption algorithms are responsible for encryption strength. We talk about bit encryption strength. Here are some of the most popular encryption algorithms.

1. Data Encryption Standard (DES) - DES

Data Encryption Standard is the original encryption standard of the US government. Initially it was said to be unbreakable but the increase in computer power and hardware costs made 56-bit encryption obsolete. This is especially true with sensitive data.

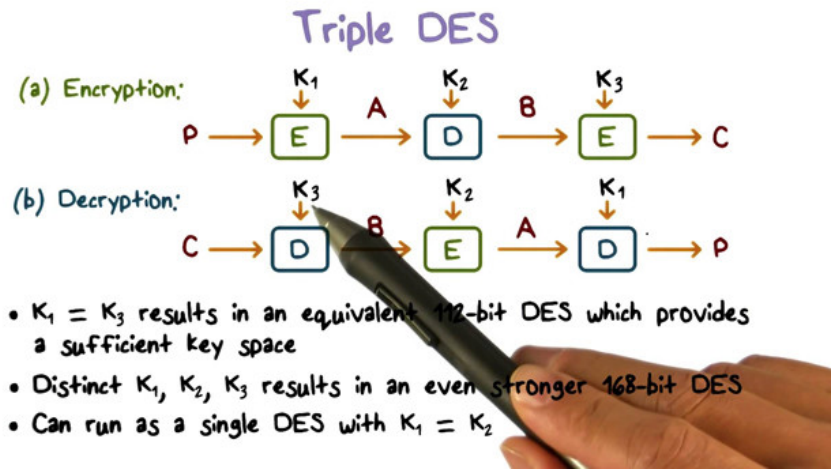


John Gilmore, co-founder of the EFF, head of the Deep Crack project, said: 'When designing safety systems and infrastructure for society, listen to cryptographers, not the main ones. therapist '. He warns users of DES encryption to store private data that record time to crack DES is short, so be careful when using it.

However, you'll still find DES in many products because it's low-level encryption is easy to do without requiring a large amount of computing power.

2. TripleDES

TripleDES (sometimes written as 3DES or TDES) is a newer, safer version of DES. When DES was cracked in less than 23 hours, people realized the problem, so this is why TripleDES was born. TripleDES speeds up the encryption process by running DES three times.



The data is encrypted, decoded and then encoded again, providing an effective key length of 168 bits. It is long enough for the most sensitive data. However, although TripleDES is longer than the DES standard, it also has errors.

TripleDES has three locking options:

1. **Option Key 1:** All three keys are independent. This method provides the strongest key strength: 168 bits.

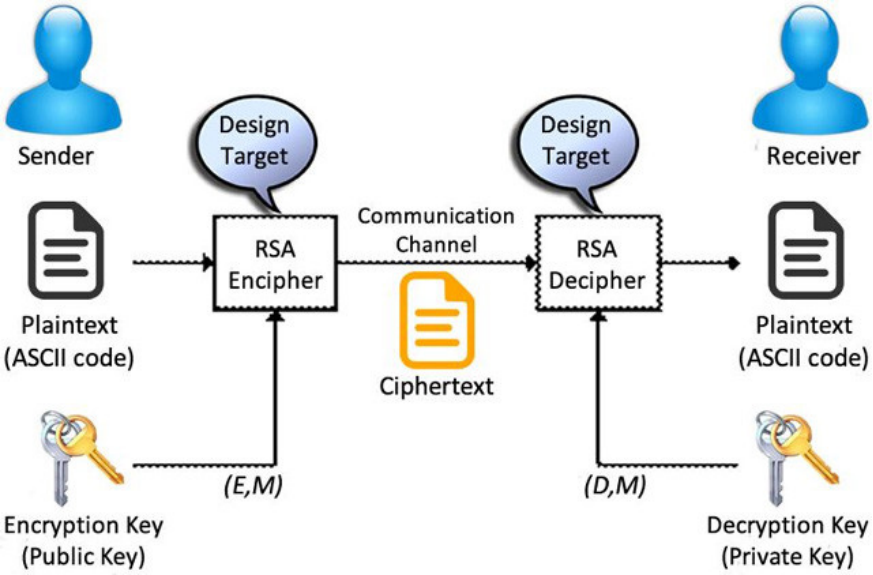
2. **Options Key 2** : Key 1 and Key 2 are independent, while Key 3 is the same as Key 1. This method provides an effective lock of 112 bits (2 × 56 = 112).

3. **Option Key 3** : All three keys are the same. This method provides a 56 bit key.

Key 1 option is the strongest. The Key 2 option is not strong, but still provides twice as much protection as DES encryption. TripleDES is a block cipher, which means that the data is encoded in a fixed block size. However, the small 64-bit TripleDES block size makes it slightly sensitive to certain attacks (such as block conflicts).

3. RSA

RSA (named after its creator Ron Rivest, Adi Shamir and Leonard Adleman) is one of the first public key encryption algorithms. It uses a one-way asymmetric encryption function.

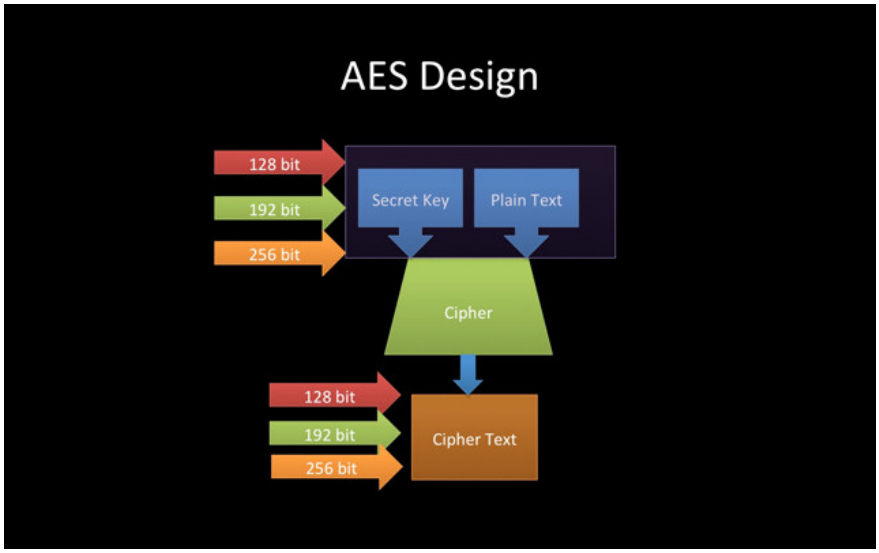


RSA algorithm is widely used on the Internet. It is the main feature of many protocols including SSH, OpenPGP, S / MIME and SSL / TLS. In addition, the browser uses RSA to establish secure communication over unsecured networks.

RSA is still very popular due to its key length. An RSA key is usually 1024 or 2048 bits long. However, security experts believe that it does not take long to crack RSA 1024 bits, so many organizations must switch to a more powerful 2048 bit key.

4. Advanced Encryption Standard (Advanced encryption standard - AES)

Advanced Encryption Standard (AES) is currently the encryption standard used by the US Government. It is based on the Rijndael algorithm developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. Belgian cryptographers sent their algorithms to the National Institute of Standards and Technology (NIST), competing with 14 other encryption algorithms to become the next type of encryption. after DES. The 'win' Rijndael and was chosen as the AES algorithm was proposed in October 2000.



AES is a symmetric key algorithm and uses symmetric block cipher. It includes three main sizes: 128, 192 or 256 bits. Moreover, there are different encoding rings for each key size. One round is the process of converting raw text into encrypted text. For 128-bit, there are 10 rounds (round); 192-bit has 12 loops, and 256-bits has 14 loops.

There are theoretical attacks against the AES algorithm, but all require specific data storage and certain time, so it is not feasible at the present time. For example, an attack on AES encryption requires 38 trillion data, more than all data is stored on all computers worldwide in 2016. Estimate the time needed to create tons of data. Brute-force public key AES-128 is billions of years.

See also: Summary of popular network attacks today

Thus, cryptographer Bruce Schneier does not 'believe that anyone can discover an attack that reads traffic Rijndael'. Schneiers' Twofish encryption algorithm (discussed below) is a direct competitor of Rijndael in the competition to choose a new national security algorithm.

5. Twofish

Twofish is the standard for being a "finalist" in the national security algorithm selection and losing to Rijndael. The Twofish algorithm works with key sizes of 128, 196 and 256 bits and has a complex key structure that makes it difficult to crack.

Security experts consider Twofish one of the fastest encryption algorithms and a great choice for both hardware and software. Moreover, Twofish passwords are free for all users. It appears in some of the best free encryption software, such as VeraCrypt (drive encryption), PeaZip (archive file) and KeePass (open source password management), as well as the OpenPGP standard.

Why not create your own encryption algorithm?

You have seen some of the best encryption algorithms, because they are basically unbreakable, at least for the time being. These cryptographic algorithms are tested with the combination of the most powerful computers and the smartest brains. New encryption algorithms undergo a series of rigorous tests.

Take the AES algorithm as an example:

1. NIST called on coders to create new encryption algorithms in September 1997.
2. NIST received 15 potential AES algorithms in August 1998.
3. At a conference in April 1999, NIST selected the last five algorithms: MARS, RC6, Rijndael, Serpent and Twofish.
4. NIST continues to check and receive comments and instructions from the cryptographic community until May 2000.
5. In October 2000, NIST confirmed Rijndael as a potential AES, then began another consultation phase.
6. Rijndael, as AES, was announced as a federal information processing standard in November 2001. Validation begins under the cryptographic algorithm approval program.
7. AES became the official government encryption standard in May 2002.

You see, coding production is really a safe, long and powerful process that takes time and in-depth analysis from some of the most powerful security organizations on the planet. Therefore, you have no resources to create a powerful algorithm. As Bruce Schneier says: 'Anyone can invent an encryption algorithm that they themselves cannot break; but it's hard to invent something that no one else can break. '

See more:

1. What is data encryption? Things to know about data encryption
2. How to be able to encrypt and protect files or folders?
3. Can data encryption protect you from Ransomware?