

Symmetric vs. asymmetric algorithms

When using symmetric algorithms, both parties share the same key for en- and decryption. To provide privacy, this key needs to be kept secret. Once somebody else gets to know the key, it is not safe any more. Symmetric algorithms have the advantage of not consuming too much computing power. A few well-known examples are: DES, Triple-DES (3DES), IDEA, CAST5, BLOWFISH, TWOFISH.

Asymmetric algorithms use pairs of keys. One is used for encryption and the other one for decryption. The decryption key is typically kept secretly, therefore called "private key" or "secret key", while the encryption key is spread to all who might want to send encrypted messages, therefore called "public key". Everybody having the public key is able to send encrypted messages to the owner of the secret key. The secret key can't be reconstructed from the public key. The idea of asymmetric algorithms was first published 1976 by Diffie and Hellmann.

Asymmetric algorithms seem to be ideally suited for real-world use: As the secret key does not have to be shared, the risk of getting known is much smaller. Every user only needs to keep one secret key in secrecy and a collection of public keys, that only need to be protected against being changed. With symmetric keys, every pair of users would need to have an own shared secret key. Well-known asymmetric algorithms are RSA, DSA, ELGAMAL.

However, asymmetric algorithms are much slower than symmetric ones. Therefore, in many applications, a combination of both is being used. The asymmetric keys are used for authentication and after this has been successfully done, one or more symmetric keys are generated and exchanged using the asymmetric encryption. This way the advantages of both algorithms can be used. Typical examples of this procedure are the RSA/IDEA combination of PGP2 or the DSA/BLOWFISH used by GnuPG.

Encryption

What is it and why is it necessary?

Goal of Encryption of Internet Traffic

- conveys confidentiality to messages while in transit
- changes readable text messages into something that cannot be read
- discourages anyone from reading or copying the messages

Related Problem

- if header information is not encrypted, traffic analysis is possible
- traffic analysis - the analysis of header information in order to derive useful information from the headers

Encryption Components

- an algorithm
- a key

Encryption Algorithms

- a series of steps that mathematically transforms plain-text or other readable information into unintelligible cipher text.
- Cipher text - Data that has been encrypted. Cipher text is unreadable until it has been converted into plain text (decrypted) with a key.

Decryption

- The inverse mathematical transformation, which transforms the encrypted cipher text back into something readable, is called decryption.

Encryption Algorithm - Input and Output

- a key and plain text are input into an encryption algorithm
- cipher text is output from the encryption algorithm

Encryption Keys

- a bit string consisting of x number of bits. A 40 bit key is a string consisting of 40 bits
- an encryption algorithm can use one of a large number of possible keys
- the number of possible keys each algorithm can support depends on the number of bits in the key. The longer the key, the more the possible number of keys

Encryption Key Example

- example - if the key length is 40, then 2 to the n , where n is the number of bits in the key, results in 1,000,000,000,000 possible key

combinations, with each different key causing the algorithm to produce slightly different cipher output

Security and Encryption

- encryption algorithms are considered secure if the security depends on only one factor - key length
- security does not depend on secrecy, inaccessibility, or anything else, only on the key length
- if this factor is true, then the only possible attack against the algorithm is a brute force attack

Brute Force Attacks and Security

- all key combinations must be tried in order to find the correct key
- the length of the key determines the possible number of keys available for selection
- the longer the key length the longer it takes to discover which key will actually decrypt
- specifying a long enough key length makes a brute-force attack non-feasible

Symmetric Encryption

- identical keys are used to encrypt and decrypt the message
- a message encrypted by one specific symmetric key can only be decrypted by using the same key, it can be decrypted with a different key

Symmetric Keys

- a random bit string, n bits long
- most often generated on the source computer

Advantages of Using Symmetric Encryption

- the encryption process is simple
- each trading partner can use the same publicly known encryption algorithm - no need to develop and exchange secret algorithms
- security is dependent on the length of the key

Drawbacks of Using Symmetric Encryption

- a shared secret key must be agreed upon by both parties

- if a user has n trading partners, then n secret keys must be maintained, one for each trading partner
- authenticity of origin or receipt cannot be proved because the secret key is shared
- management of the symmetric keys becomes problematic

Problems with Management of Symmetric Keys

- trading partners must always use the exact same key to decrypt the encrypted message
- key exchange is difficult because the exchange itself must be secure with no intervening compromise of the key
- management of keys is difficult as numbers of trading partners increases, especially when multiple keys exist for each trading partner

Public Key Cryptography as a Solution for Managing Symmetric Keys

- public key cryptography simplifies the management of symmetric keys to the point whereby a symmetric key can be used not only for each trading partner, but for each exchange between trading partners
- additionally, public key cryptography can be used to unambiguously establish non-repudiation of origin and receipt

Asymmetric Encryption - (Public Key Cryptography)

- based on the concept of a key pair
- each half of the pair (one key) can encrypt information that only the other half (one key) can decrypt
- the key pair is designated and associated to one, and only one, trading partner

Asymmetric Key Pairs

- consists of two keys - one private and one public
- private key is secret and only known by the designated trading partner it belongs to
- public key is published widely but still associated only with the designated trading partner

Asymmetric Key Uses

- confidentiality
- digital signatures
- both uses depend on the association of a key pair with one, and only one owner of the keys
- both uses depend on one of the keys in the key pair being secret from everyone but the owner of the key

Confidentiality Using Asymmetric Key Pairs (Encryption)

- Trading Partner A desires to send a confidential message to Trading Partner B
- Trading Partner A retrieves Trading Partner B's public key and encrypts the message with it

Confidentiality Using Asymmetric Key Pairs (Decryption)

- Trading Partner B receives the message and decrypts the message with the secretly held, private key
- The only key that can possibly decrypt a message that is encrypted with Trading Partner B's public key is Trading Partner B's private key

Digital Signatures Using Asymmetric Key Pairs (Encryption)

- Trading Partner A desires to send a digitally signed message to Trading Partner B
- Trading Partner A uses their own private key to encrypt a part of the message
- Trading Partner A sends the encrypted part of the message to B

Digital Signatures Using Asymmetric Key Pairs (Decryption)

- Trading Partner B receives Trading Partner A's message and obtains A's public key
- Trading Partner B tries to decrypt the encrypted portion of Trading Partner A's message
- If it decrypts, Then Trading Partner B knows it has to be from A because the only thing A's public key will decrypt is something encrypted with A's private key and only A has access to that private key

Real World Usage of Asymmetric Encryption

- public key encryption algorithms are considerably slower than symmetric key algorithms
- rarely used as encryption methodology for bulk messages or parts of messages
- normally used in conjunction with a Message Integrity Check (MIC) or to encrypt a symmetric key, where the MIC or symmetric key is what is encrypted using public key encryption algorithms

Speed Comparison - Symmetric vs Asymmetric

- software encryption using DES (symmetric key algorithm) is 100 times faster than software encryption using RSA (asymmetric key algorithm) - estimate provided by RSA Data Securities
- hardware encryption using DES (symmetric key algorithm) is anywhere from 1,000 to 10,000 times faster than hardware encryption using RSA (asymmetric key algorithm)

Encryption Needs for Confidential Commercial Exchanges

- for interoperability between two trading partners
- standard encryption algorithm(s)
- standard key length(s)
- agreed upon beforehand or within an individual transaction

Issues

- how secure is the algorithm?
- how fast are current implementations of the algorithm?
- availability of APIs and/or tools to implement the algorithm
- frequency of use of algorithm with other trading partners
- sufficient key length to discourage brute force attacks

Common Symmetric Key Algorithms

- Data Encryption Standard - DES
- Triple DES
- RC2 and RC5
- IDEA

Block Ciphers vs Stream Ciphers

- block ciphers - take a set number of bits, typically 64 bits, and encrypts them as a single block
- stream ciphers - take and encrypt one bit at a time
- Most ciphers belong to the block cipher class.

Data Encryption Standard - DES

- most widely used commercial encryption algorithm
- in the public domain, available to all
- a U. S. government encryption standard
- security is known and is dependent solely on the key length
- data sequenced into 64 bit blocks prior to encryption, each block encrypted

Cipher Block Chaining (CBC)

- recommended mode for using DES
- each 64 bit block of data is exclusively OR'd with the previous block before encryption
- gives added protection by making each cipher-text block depend on each other
- changes in the cipher text can be detected

Brute Force Attacks against DES

- DES specifies a 56 bit key, so there are 2 to the 56th possible keys
- brute force attack means trying every single key (10,000,000,000,000,000) to decrypt 8 bytes of known cipher text into the corresponding plain text

Resources Required to Break DES Key

- \$1 million dollar hardware based, brute-force attack on DES takes approximately 3.6 hours to recover the DES key
- \$1 million dollar software based, brute force attack on DES takes approximately 3 years to recover the DES key
- above figures attributed to B. Schneier, "E-Mail Security", John Wiley & Sons, 1995

Triple DES

- variant on DES which encrypts message 3 times with 2 independent 56 bit keys
- effective key length is 112 bits
- brute force attack on Triple DES is not feasible

RC2 and RC5

- RSA owned proprietary symmetric key algorithms
- variable key length makes security configurable
- RC2 is a block cipher (similar to DES) and should be used in CBC mode, RC5 is also a block cipher and should be used in CVC Pad mode
- Both use 128 bit key but support key masking for configuration of key length

International Data Encryption Algorithm (IDEA)

- a block cipher, in the mold of DES
- uses a 64-bit block size and a 128-bit key
- IDEA in CBC mode is the bulk encryption algorithm used by Pretty Good Privacy (PGP) which makes it the most widely used encryption algorithm for

Key Lengths and Secure Transactions

- Algorithms that make a brute force attack not feasible
- Triple DES with 2 56 bit keys
- RC2 and RC5 with 128 bit keys
- IDEA with 128 bit key

Recommendations on Key Lengths

- Transactions of minimal or small value - 40 bit RC2 or 56 bit DES
- Most commercial applications need a key length of 75 bits
- High value transactions Triple-DES, IDEA or 128 bit RC2 or RC5

Conclusions

- Encryption is the correct method to implement confidentiality for Internet traffic
- Symmetric key algorithms should be chosen for encryption of confidential data
- The more bits in the symmetric key, the less probable the compromise of the encrypted data