Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

PGP: A Hybrid Solution

Cryptography is the science of keeping data secure. Encryption is the process of using cryptography to encode data so that it's meaning is not immediately obvious. There are two main types of cryptography that are used, symmetric and asymmetric. It is also possible to use a hybrid of the two; Pretty Good Privacy (PGP) by Network Associates is an example of this. Symmetric and asymmetric cryptography both have advantages and disadvantages that will be discussed in this paper. PGP brings the best of each together and als...

Copyright SANS Institute
Author Retains Full Rights

AD
ONLY ONE INDEPENDENT TEST
MEASURES REAL-WORLD,
ENDPOINT MALWARE PROTECTION.
TREND MICRO SMART PROTECTION NETWORK

PGP: A Hybrid Solution

Jessica J. Benz
GIAC Certification Version1.2e

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Cryptography is the science of keeping data secure. Encryption is the process of using cryptography to encode data so that it's meaning is not immediately obvious. There are two main types of cryptography that are used, symmetric and asymmetric. It is also possible to use a hybrid of the two; Pretty Good Privacy (PGP) by Network Associates is an example of this. Symmetric and asymmetric cryptography both have advantages and disadvantages that will be discussed in this paper. PGP brings the best of each together and also works to minimize the disadvantages. This will also be discussed. Alice and Bob are often used as examples when cryptography is explained, therefore I will also use them for most examples.

Cryptographic Terms

First some cryptographic terms must be defined.

- Plaintext is unencrypted data, and will be referred to by M
- Ciphertext is encrypted data, and will be referred to by C.
- The process of encrypting data is referred to by E.
- The process of decrypting data is referred to by D.
- Keys are represented by K
- E(M)=C
  - Cipher-text C is output of the encryption of plain-text M
- D(C)=M
  - Plain-text M is the output of the decryption of the cipher-text C

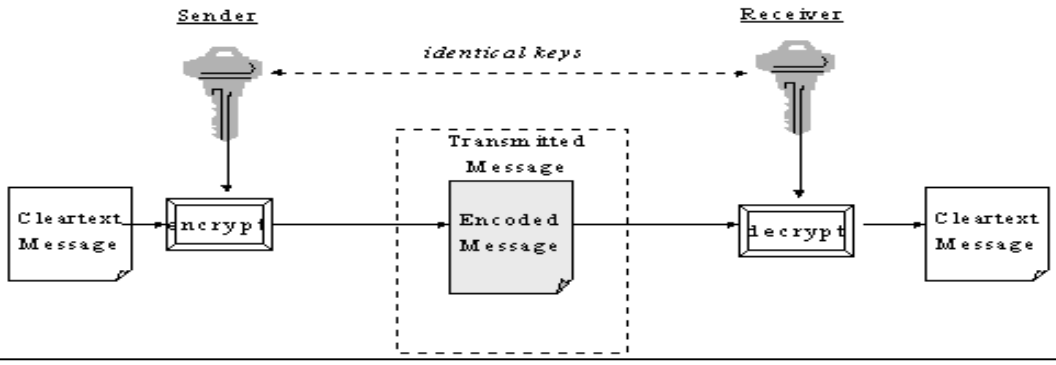
Given the above, the following must be true.

- D(E(M))=M
  - Plain-text M is the output of the decryption of the encrypted plain-text M.

Symmetric Encryption

Symmetric cryptography, also known as conventional or secret encryption, is when the encryption and decryption keys are the same value. An example of symmetric cryptography is the Caesar Cipher. When Alice and Bob want to exchange data, they must first decide upon an algorithm such as the Caesar Cipher. Alice first writes her message in plaintext, then shifts each letter of her message 3 characters to the left. So, A becomes D, B becomes E, and so on. Bob knows in order to decrypt the data, he shifts each ciphertext letter back 3 characters, this then reveals the plaintext. Both Alice and Bob know that shifting each letter the appropriate direction is the key. Symmetric encryption is also known as a shared secret cryptography or shared key cryptography because it uses a single "shared" key that is used to encrypt and decrypt the message. Symmetric encryption is represented mathematically by: $D_K(E_K(M))=M$. The diagram below represents symmetric encryption graphically.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.



http://www.rowan.edu/business/faculty/hamilton/seminar/presentations/encryption/sld006.htm

There are many advantages and disadvantages to using symmetric encryption.

Advantages to using symmetric encryption:

- ✓ Provides authentication, as long as the key stays secret.
- ✓ Data is encrypted very quickly.
- ✓ Symmetry of key allows encryption and decryption with same key.

Disadvantages to using symmetric encryption:

- ⊘ If the key is revealed (lost, stolen, guessed, etc) the interceptors can immediately decrypt anything that was encrypted using the key. An imposter using an intercepted key can produce bogus messages by impersonating the legitimate sender.

  Solution:

  - ➢ Change keys frequently
    - ⌧ Not feasible in most situations, especially in large groups.

- ⊘ Distribution of keys becomes a problem, especially if keys change frequently. Keys must be transmitted with extreme security because they allow access to all the information encrypted with them. For applications that extend throughout the world, this can be a very complex task.

  Solutions:

  - ➢ Face-to-face key exchange.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Not feasible in most situations, especially when large groups are exchanging keys
- Use couriers for key exchange
  - Can couriers really be trusted?
- Split key distribution,
  - If one part is intercepted it is likely that additional parts will also be intercepted.
  - Even if one part of the key is distributed through email, and the other part through voicemail, both are still vulnerable to attack.

- The number of keys increases with the square of the number of people exchanging secret information. For example, Alice needs a key for every person/group she is exchanging information with; Alice cannot use the same key for two different people/groups. The total number of keys that Alice needs can be represented as N= n*(n-1)/2, where N is the number of keys needed and n is the number of people exchanging data; so when n=3, N=3, when n=4, N=6, and when n=10, N=45. If Alice were exchanging information with Bob, Carol, Dan, Edith, Faye, Gail, Homer, Isabel, and Jason, she would need 45 keys.

Alice ⇔ Bob	Bob ⇔ Isabel	Edith ⇔ Faye
Alice ⇔ Carol	Bob ⇔ Jason	Edith ⇔ Gail
Alice ⇔ Dan	Carol ⇔ Dan	Edith ⇔ Homer
Alice ⇔ Edith	Carol ⇔ Edith	Edith ⇔ Isabel
Alice ⇔ Faye	Carol ⇔ Faye	Edith ⇔ Jason
Alice ⇔ Gail	Carol ⇔ Gail	Faye ⇔ Gail
Alice ⇔ Homer	Carol ⇔ Homer	Faye ⇔ Homer
Alice ⇔ Isabel	Carol ⇔ Isabel	Faye ⇔ Isabel
Alice ⇔ Jason	Carol ⇔ Jason	Faye ⇔ Jason
Bob ⇔ Carol	Dan ⇔ Edith	Gail ⇔ Homer
Bob ⇔ Dan	Dan ⇔ Faye	Gail ⇔ Isabel
Bob ⇔ Edith	Dan ⇔ Gail	Gail ⇔ Jason
Bob ⇔ Faye	Dan ⇔ Homer	Homer ⇔ Isabel
Bob ⇔ Gail	Dan ⇔ Isabel	Homer ⇔ Jason
Bob ⇔ Homer	Dan ⇔ Jason	Isabel ⇔ Jason

Now imagine you have a company with 100 people, each person would have to have 4,950 keys to exchange information using symmetric key encryption!

Solutions:

- Have only a few people exchange data that needs to be encrypted directly over the network.
  - Not feasible in most situations.
- Use a central clearinghouse, which accepts the encrypted information from one party, decrypts it with the receiving parties key and sends it on.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- This then becomes a point of attack.
- Use asymmetric (public key) cryptography.

- Symmetric keys are subject to a brute force attack where all keys in the key space are tried systematically to break the encryption

Solution:

- Use asymmetric (public key) encryption

Asymmetric Encryption

Asymmetric encryption, also known as public key encryption, is encryption that uses two different keys for encryption and decryption. One key is a public key that can be distributed to anyone. The other is a mathematically related key called a private key or secret key. This is a key that should be kept secret from the world. Only the owner should have access to the private key or any back-up copies of it. One should protect his/her secret key in the same manner that they would treat their bank PIN or credit card information.

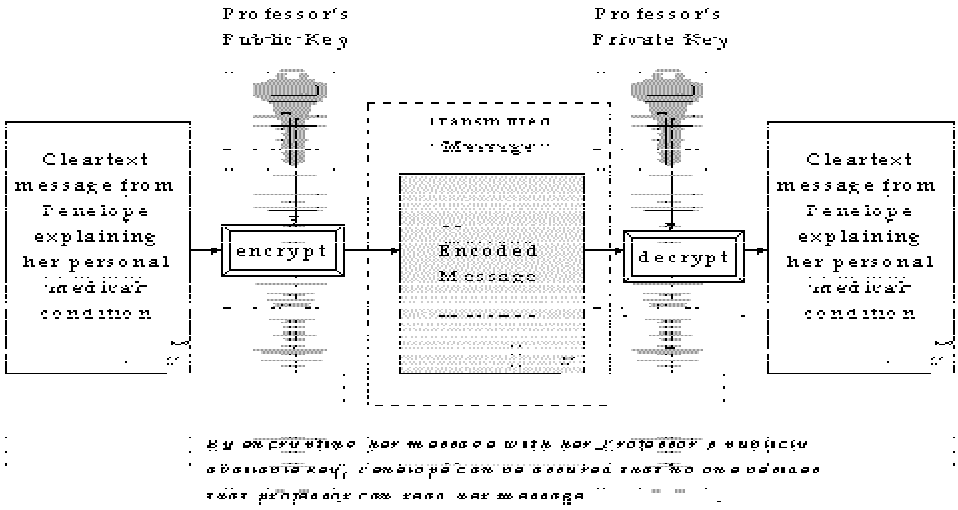
Each user has two keys, public and private

$$D_{Kpublic}(E_{Kprivate}(M))=M$$

Sometimes we also want

$$D_{Kprivate}(E_{Kpublic}(M))=M$$

This would be used when Alice is signing data that is sent to Bob. Alice uses her private key to sign the message so Bob can verify the signature with Alice's public key, to confirm that the data has not been tampered with.



http://www.rowan.edu/business/faculty/hamilton/seminar/presentations/encryption/sld010.htm

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Advantages to using asymmetric encryption

- ✓ For any number n users (represented as "n"), only 2*n, (N=2*n) keys are required instead of n*(n-1)/2 as with symmetric encryption. In other words when n=3, N=6, when n=4, N=8, and when n=10, N=20. In asymmetric encryption, each user only has 1 key pair. This means only a person's public key is exchanged and each group of people do not need separate keys.
- ✓ The problem of distributing keys is solved because a user's public key can be shared by anyone.

Disadvantages to using asymmetric encryption

- ⊘ Only a few public key algorithms are both secure and practical
- ⊘ Some algorithms are only suitable for key distribution
- ⊘ Slow: 100-1000 times slower than symmetric algorithms (RSA v. DES)
- ⊘ Only three algorithms work well for both key distribution and encryption:
  - RSA
  - ElGamal
  - Rabin

The most commonly used are RSA and ElGamal.

Solution:

- ➢ Use a hybrid system like Pretty Good Privacy (PGP).

Pretty Good Privacy (PGP)

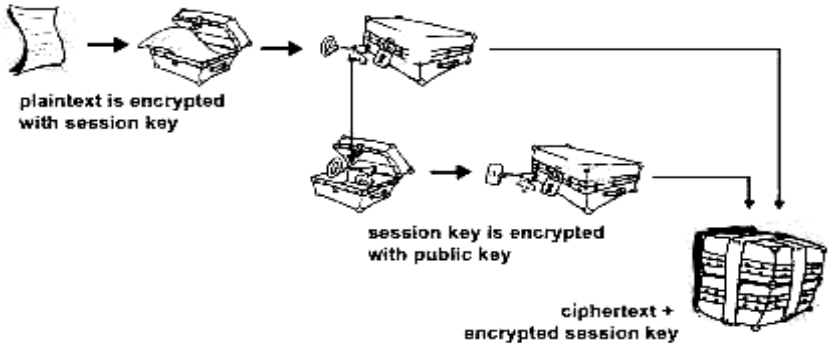
PGP combines the advantages of both asymmetric and symmetric encryption, while also downplaying the disadvantages of both.

How PGP works

When a user encrypts plaintext with PGP, PGP first compresses the plaintext. Data compression, among other things, strengthens cryptographic security because it reduces the patterns found in languages. PGP then creates a session key; this key is a random number generated from the movements of the user's mouse and the keystrokes he/she types. Then the random number is run through a symmetric encryption algorithm such as Triple DES, Twofish, CAST, or AES (Rijndael), which generates a one-time-only secret key. If there is not enough information gathered a window will pop up asking the user to move his/her mouse and type on the keyboard until sufficient random data have been gathered. The session key works with a very secure, fast conventional (symmetric) encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the

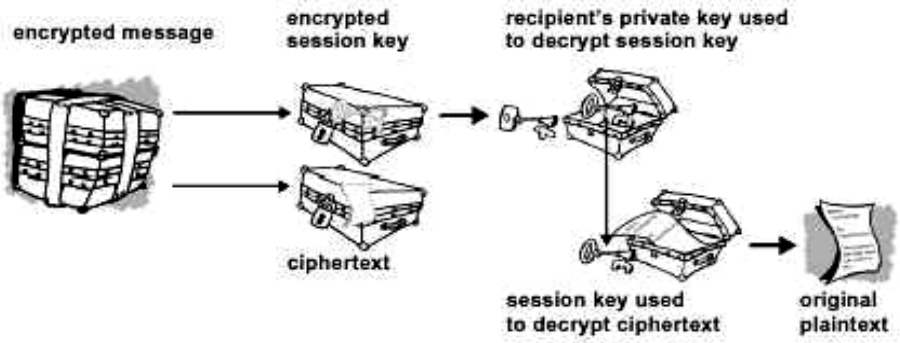
© SANS Institute 2001, Author retains full rights

recipient's public key, using asymmetric encryption such as Diffie-Hellman or RSA. This public key-encrypted session key is transmitted along with the ciphertext to the recipient. See diagram below.



ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/PGPWinUsersGuide.pdf

Decryption works in the reverse. The recipient's copy of PGP uses his or her private key to recover the session key, which PGP then uses to decrypt the conventionally (symmetrically) encrypted ciphertext. See diagram below.



ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/PGPWinUsersGuide.pdf

Advantages to Using PGP

- ✓ The combination of these two encryption methods combines the convenience of public-key encryption with the speed of conventional encryption.
- ✓ Using Conventional encryption is about 100 to 1,000 times faster than public-key encryption, which solves the problem of slow encryption with asymmetric algorithms.
- ✓ Public-key encryption provides a solution to key distribution and data transmission issues when using symmetric encryption.
- ✓ When used together, performance and key distribution are improved without any sacrifice in security.
- ✓ PGP is good hybrid solution; it ties together the advantages of public key and symmetric cryptography, while also providing a feasible solution to the disadvantages of both.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Disadvantages to Using PGP

- Using PGP can be a complex process and its concept is often difficult for some people to grasp.

  Solution:

  - Provide more training for users.

- Both parties must be able to use PGP -- It is impossible to use PGP unless people at both ends of the connection are capable of using some version of PGP.

  Solution:

  - Use a self-decrypting archive (SDA), which creates an executable file that uses conventional, symmetric encryption. This feature is available with the newer versions of PGP.

- Key management is a challenge at first within the program and can be a little awkward for users to learn.

  Solution:

  - Provide more training for users.

PGP has its advantages and disadvantages; many of the disadvantages to PGP can be overcome with thorough training and use. The advantages to using PGP far outweigh the disadvantages.

PGP is a powerful hybrid cryptosystem that combines the advantages of both symmetric and asymmetric cryptography. At the same time, PGP minimizes the disadvantages of each system.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Works Cited

An Introduction to Cryptography. ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/IntroToCrypto.pdf (June 27, 2001).

Atreya, Mohan. Introduction to Cryptography. http://www.rsa.com/solutions/developers/whitepapers/IntrotoCrypto.pdf (June 27, 2001).

Hamilton, Diane. Encryption, Authentication & Public Key Infrastructure. November 20, 2000. : http://www.rowan.edu/business/faculty/hamilton/seminar/presentations/encryption/sld006.htm (June 27, 2001)

Hamilton, Diane. Encryption, Authentication & Public Key Infrastructure. November 20, 2000. : http://www.rowan.edu/business/faculty/hamilton/seminar/presentations/encryption/sld010.htm (June 27, 2001)

Oconnort@nyu.edu. Why Encrypt?. February 10, 1997. http://www.nyu.edu/acf/staff/oconnort/why-encrypt.html (June 28, 2001).

Parviainen, Roland. Introduction to Encryption and Information Hiding. http://www.sm.luth.se/csee/courses/smd/102/lek2/lek2.html (June 27, 2001).

Parviainen, Roland. Advanced Encryption. http://www.sm.luth.se/csee/courses/smd/102/lek3/lek3.html (June 27, 2001).

Parviainen, Roland. Advanced Encryption. http://www.sm.luth.se/csee/courses/smd/102/lek4/lek4.html (June 27, 2001).

Pfleeger, Charles P. *Security in Computing*. Upper Saddle River, NJ: Prentince Hall PTR, 1997. 21-133.

PGP Freeware for Windows 95, Windows 98, Windows NT, Windows 2000, and Windows Millennium. ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/PGPWinUsersGuide.pdf (June 27, 2001).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced