Public Key Cryptography & PGP

Jay D. Dyson, Computer Systems Specialist

> ***"If you think cryptography can solve your problem, then you don't understand your problem and you don't understand cryptography."***
>
> ***-- Bruce Schneier***

Overview of Cryptography

What *is* Cryptography?

- Cryptography is an often misunderstood and misused security tool. Today more than ever, privacy is a necessary part of business communications. The following is an overview of public key cryptography and one of its more widely-used implementations, Pretty Good Privacy (PGP).

Overview of Cryptography

Terminology

- **Cryptographic/Cipher System -** A method of disguising a message so only authorized users may read it.
- **Cryptology -** The study of cryptography.
- **Encryption -** The process of converting plaintext into ciphertext.
- **Decryption -** The process of converting ciphertext back to its original plaintext.
- **Cryptographic Algorithm -** The computational procedure used to encrypt and decrypt messages.
- **Cryptanalysis -** The process of finding a weakness in, or actual breaking of, a cryptographic system.

Overview of Cryptography

What's the point?

- **Privacy -** Would you be willing to send all of your correspondence through the U.S. Mail on the back of a postcard for all to read?
- **Data Integrity -** Provides assurance that a message or file has not been altered
- **Source Authentication -** Provides a method to identify the originator of a message or file

Types of Cryptographic Systems

Secret Codes

- The simplest and oldest way to send a secret message to someone. The code must be known to the sender or recipient.

Code Phrase	True Meaning
My coffee is cold	**Launch the missiles**
Pass the cream	**Don’t launch the missiles**

Types of Cryptographic Systems

Ciphers

- Substitution ciphers are the simplest type of cipher system.
- Each letter of the alphabet is assigned to a number or different letter.
- ROT13 is a commonly used cipher.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	A	B	C	. . .

Types of Cryptographic Systems

One-Time Pads

- One-Time Pads uses a different key for a specific time period.
- Truly secure, no patterns evolve.
- Most vulnerabilities due to human carelessness.

One-Time Pad - Shift each encrypted letter x places to the right

14 07 09 06 10 02 25 13 17 08 15

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Encrypted Message

fazmyqbgnke

Decrypted Text

This is a test

Crypto Keys & Algorithms

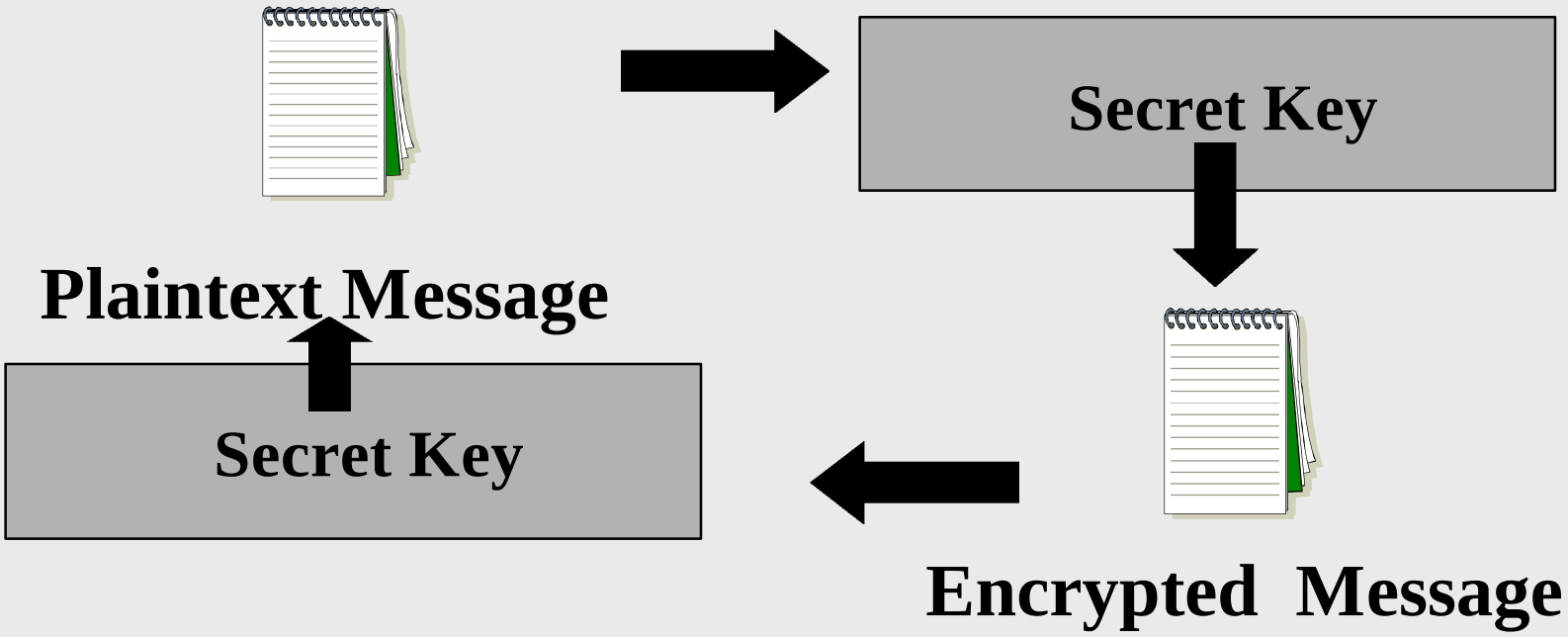
General Concepts and Definitions

- As a password is used to access a computer system, a cryptographic key is a password or passphrase that is used to unlock an encrypted message.
- Different encryption systems offer different key lengths - Just as a longer password provides more security (WindowsNT excluded) the longer and more complex the key is, the more security an encryption system provides.
- A cryptographic algorithm is a mathematical function used for encryption and decryption. Most algorithms contain a certain number of “rounds.” This determines how many times the text will be run through the algorithm

Cryptographic Methods

Secret Key (symmetric) Cryptography

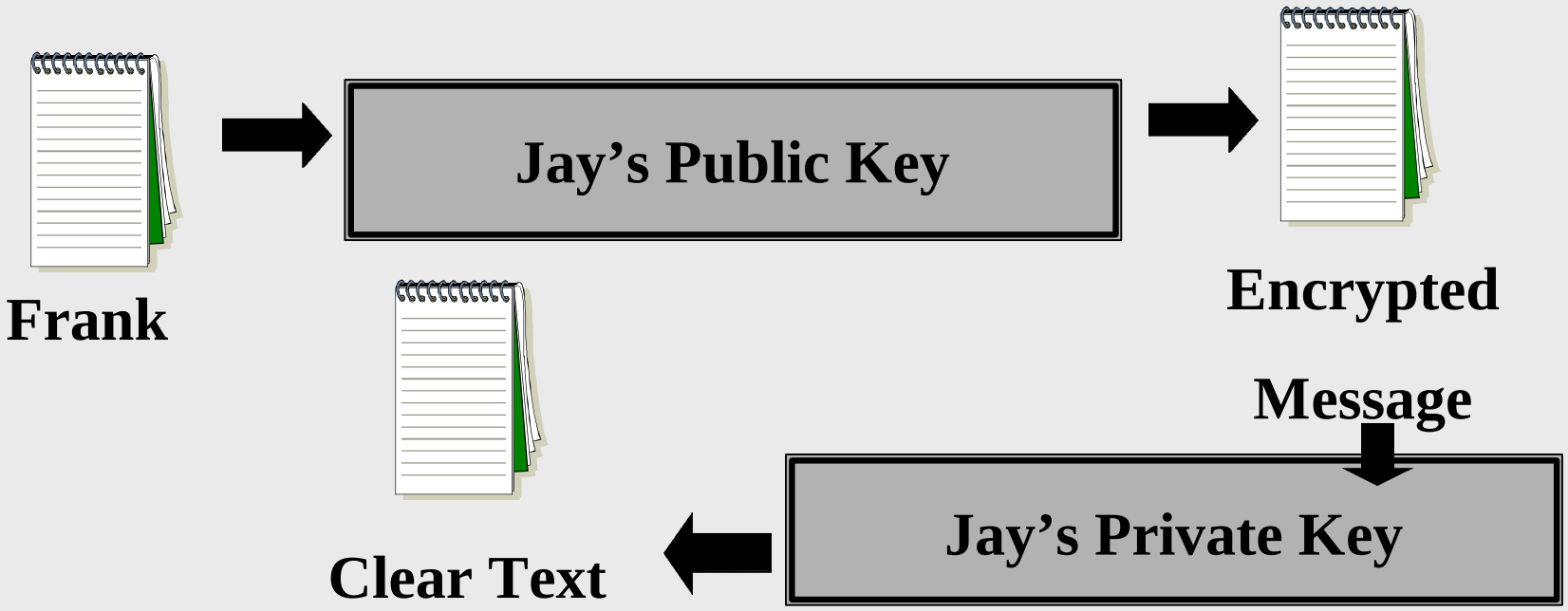
- A single key is used to both encrypt and decrypt a message. A secure channel must be in place for users to exchange this common key.



Cryptographic Methods

Public Key (asymmetric) Cryptography

- Two keys are used for this method, the public key is used to encrypt. The private key is used to decrypt. This is used when it isn't feasible to securely exchange keys.

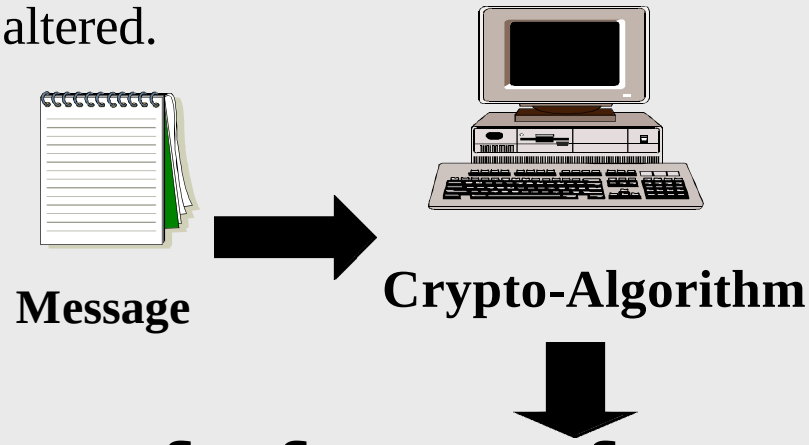


Cryptographic Methods

One-Way Functions

- **One-way functions:**

  Used to generate a fixed-length hash (also known as a message-digest) of a file. This hash is essentially a ‘digital fingerprint’ of the file that would be sent along with a document. The recipient would use the same method to generate a hash. If the hashes do not match the file has been altered.



History of Public Key Crypto

In the beginning...

1976 Whitfield Diffie and Martin Hellman publish "*New Directions in Cryptography*" which introduced the idea of public key crypto systems. They also introduce the idea of authentication by the use of a one way function.

1977 Ronald L. Rivest, Adi Shamir and Leonard M. Adleman develop a practical public key system (RSA). It was this cipher that could be used for both confidentiality and digital signatures.

Pretty Good Privacy (PGP)

Overview & History

- PGP is a personal high-security cryptographic software application that allows people to exchange messages or files with privacy, authentication, and convenience. PGP can be used to encrypt and digitally sign files and e-mail.
- Developed by Phil Zimmerman in the mid ‘80s.
- First version released on the Internet in 1991; got immediate NSA attention and encountered legal issues on its use of RSA and Merkle-Hellman cryptography patents.
- Purchased by ViaCrypt in 1993 (they had RSA license). Re-released in 1994 with RSAREF toolkit license.
- Purchased by Network Associates in 1998.

Pretty Good Privacy (PGP)

Versions

- PGP v2.6.2 (MIT PGP) is the current version for DOS/UNIX platforms for use within the U.S. (v2.6.3i is for use outside the U.S.)
- PGP v5.x freeware is also available for DOS/Windows/ UNIX platforms although it is generally regarded as not as secure as v2.x. Additionally, the v5.x freeware version is not backward compatible with PGP v2.x.
- PGP v6.x (NAI PGP) is the current commercial product which offers “PGP Desktop Security,” “PGP Personal Privacy,” and “PGP Freeware.” (The freeware version is not backward-compatible with MIT PGP.)

Pretty Good Privacy (PGP)

Why Use It?

- **Privacy -** Store and transmit your data so that only select people may view their contents.
- **Integrity -** Ensure your files, data, and applications have not been modified without your consent.
- **Authentication -** A way to verify that people actually are who they claim to be.

Pretty Good Privacy (PGP)

Basic Usage & Key Management

- **To encrypt file with recipent's pubkey: pgp -e textfile her_userid [other userids]**
- **To sign a file with your secret key: pgp -s textfile [-u your userid]**
- **To sign a file with your secret key, and encrypt it with recipent's pubkey: pgp -es textfile her_userid [-u your_userid]**
- **To decrypt or check a signature for a ciphertext (.pgp) file: pgp ciphertextfile**
- **To produce encryption/signature output in ASCII for email, add the -a option to above options.**
- **To generate your own unique public/secret key pair: pgp -kg**
- **To add a key file's contents to your public or secret key ring:pgp -ka keyfile [keyring]**

Pretty Good Privacy (PGP)

Basic Use & Key Management (Continued)

- **To remove a key or a user ID from your public or secret key ring: pgp -kr userid [keyring]**
- **To edit your user ID or pass phrase:**
  pgp -ke your_userid [keyring]
- **To check signatures on your public key ring:**
  pgp -kc [userid]
- **To sign someone else's public key on your public key ring:**
  pgp -ks her_userid
- **To view the contents of your public key ring:**
  pgp -kv

Pretty Good Privacy (PGP)

Generating a Key

- To create a new key: **`pgp -kg`**
- Select option 3: **`1024 bits-"Military" grade, slow, highest security`**
- Enter a user ID for the new key (usually name followed by email address: **`Joe Public <jpublic@public.com>`**
- Enter a pass phrase. This phrase is used to encrypt your secret key.
  * do not use the same password or pass phrase that is used on another system
  * do not use common words or proper names
  * do not use any single word that may be contained in a dictionary

Pretty Good Privacy (PGP)

Generating a Key

- Use an actual phrase and not just a single password.
- Example of a good pass phrase: “Sew ewe theenk ewe kan haq mie passfraze bye heereeng mee saye it 2 tymez?”
- NOTE: passphrases are *case-sensitive*!
- Do not use lines from history, popular movies or books!
- The last step is to input random text in order to generate a series of random bits. This is done by measuring the time intervals between keystrokes.
- The random bits are used to create the user’s keys.
- The generated keys will be placed on your public and private keyrings.

Pretty Good Privacy (PGP)

PGP Public Key Certificates

- PGP stores each public key in a key certificate which contains:
  - The public key itself.
  - The ID of the key's creator (usually name & email address).
  - The date the key was created & expiration date.
  - A list of digital signatures provided by people who attest to the key's authenticity.

Pretty Good Privacy (PGP)

Encrypting & Decrypting Files

- To encrypt a file with a recipient's public key:
  `pgp -e <filename> <user ID>`
- This will produce the file **`filename.pgp`** Only the recipient can decrypt the file using their private key.

Note: Whenever encrypting text files to send via the Internet also use the 'a' option for ***ASCII*** output

- The recipient can decrypt the file with:
  `pgp filename.pgp`
- They will then be prompted to enter their private key pass phrase.

Pretty Good Privacy (PGP)

Digital Signatures

- To add a digital signature to a file:
  `pgp -sta filename`
- The user will be prompted to enter their pass phrase.
- The file <filename.asc> will be created which contains the digital signature of the sender.
- The recipient can verify the digital signature to ensure the files contents have not changed: **`pgp filename.asc`**

Pretty Good Privacy (PGP)

Digital Signatures

- The recipient will be notified if the file has a good signature:

```
Good signature from user "Joe Public<jpublic@public.com>".
Signature made 1998/07/27 04:29 GMT
```

- If the file had been modified even by one byte the recipient would be advised that the signature was not valid:

```
Bad signature from user "Joe Public <jpublic@public.com>".
Signature made 1998/07/27 04:29 GMT
```

PGP Enhancements

General Notes

- Utilities and filters are available that make PGP easier to use for the end-user. (Please see *http://techreports/~jdyson/pgp4pine/index.html*)
- NAI PGP functions as a plug-in to Eudora and other popular Mail User Agents (MUAs). NAI PGP also has a number of disk utilities for digital signatures and encryption.
- There is also PGPfone for voice communications, but that's another story altogether...

Public Key Crypto & PGP

Suggested Reading

- **Applied Cryptography** (Bruce Schneier)
  John Wiley & Sons, 1996 - ISBN: 0-47111-709-9
- **Attrition.Org Cryptography Archives**
  http://www.attrition.org/~wrlwnd/crypto/
- **International PGP Home Page**
  http://www.pgpi.org/
- **MIT PGP Home Page**
  http://web.mit.edu/network/pgp.html
- **NAI PGP Home Page**
  http://www.pgp.com/
- **PGP - Pretty Good Privacy** (Simson Garfinkel)
  O'Reilly & Associates, 1995 - ISBN: 1-56592-098-8
- **PGP RSA vs. PGP DH/DSS FAQ**
  http://www.scramdisk.clara.net/pgpfaq.html