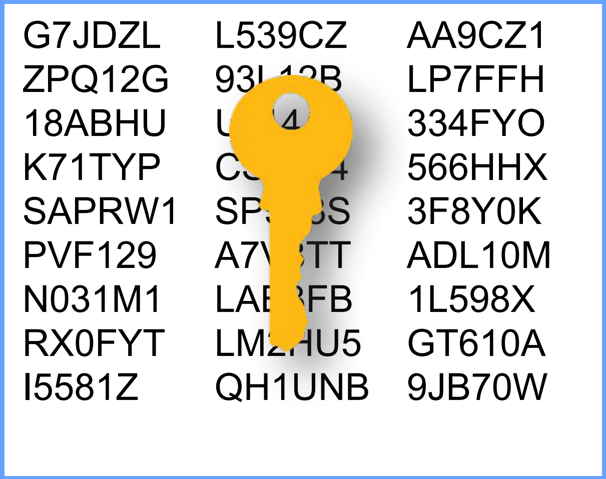
CORK INSTITUTE OF TECHNOLOGY

INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

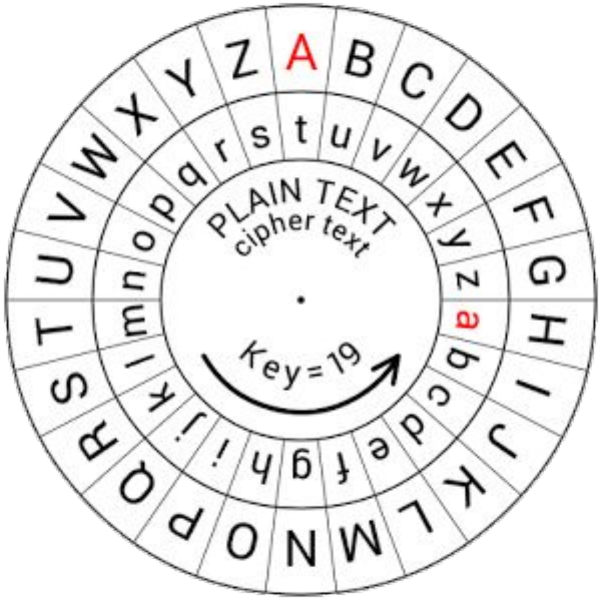
Computer Security Principles



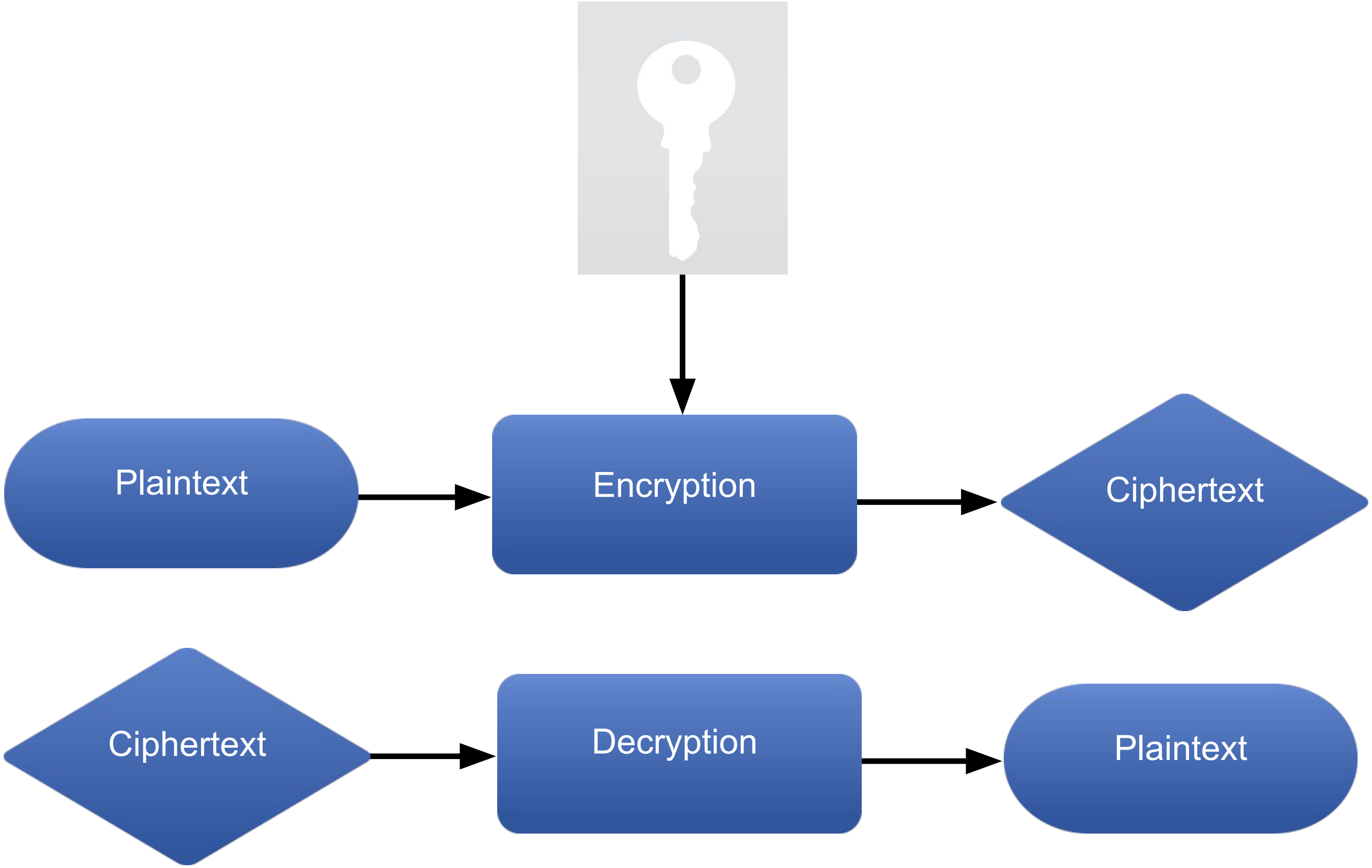
Lecture 12: Cryptography

Classical Encryption

- A long time ago when Julius Caesar was sending messages to his generals, he didn't trust his messengers.
- So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the "shift by 3" rule could decipher his messages.
- This was the earliest known use of a substitution cipher.


PLAIN TEXT
cipher text
Key=19
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
t u v w x y z a b c d e f g h i j k l m n o p q r s

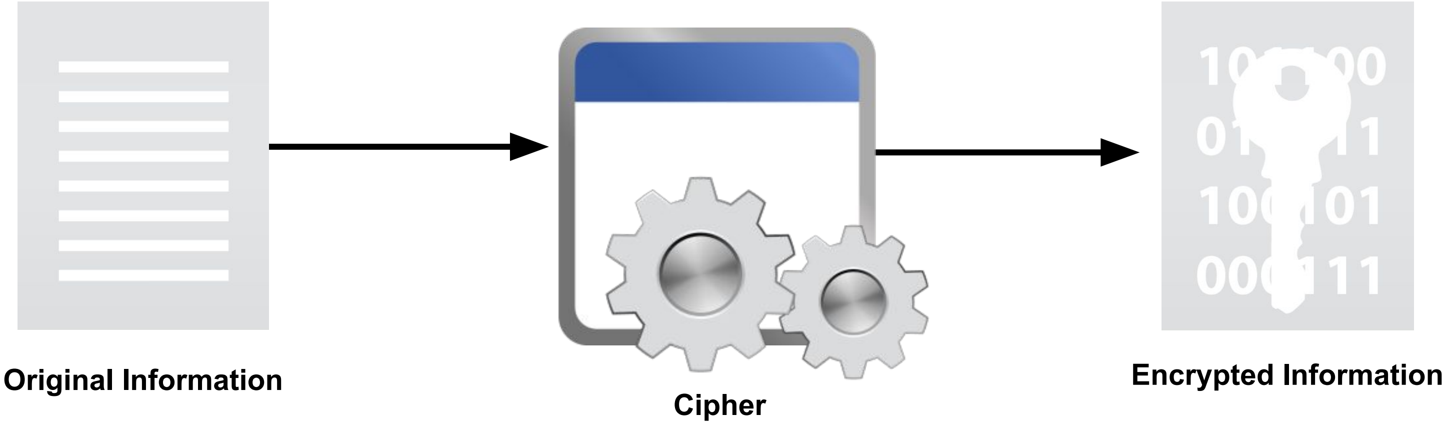
Encryption and Decryption



Encryption and Decryption

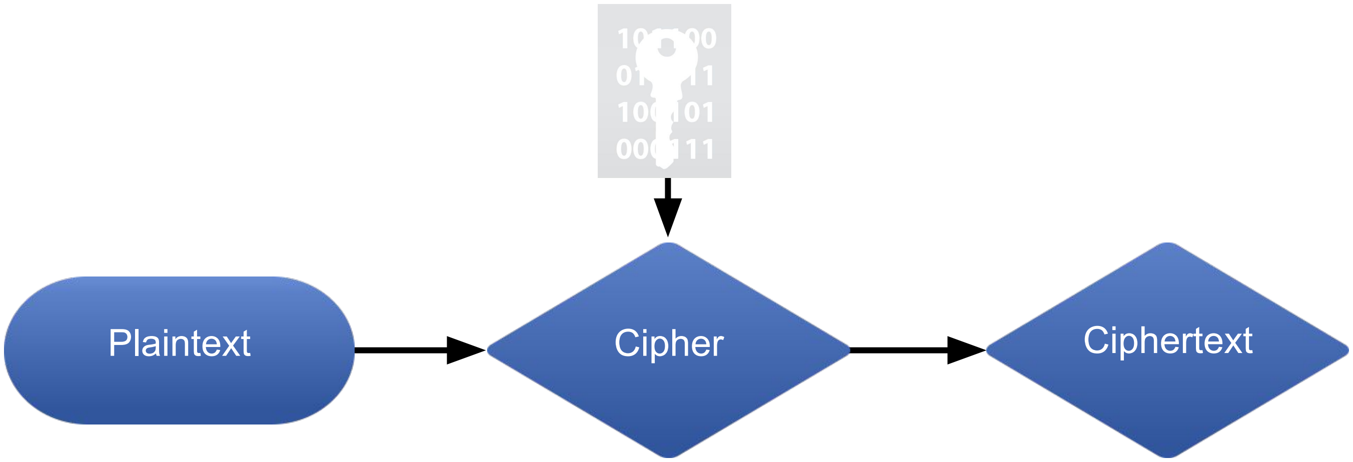
- Data that can be read and understood without any special measures is called plaintext or cleartext.
- The method of disguising plaintext in such a way as to hide its substance is called encryption.
- Encrypting plaintext results in unreadable gibberish called ciphertext.
- You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data.
- The process of reverting ciphertext to its original plaintext is called decryption.

Ciphers

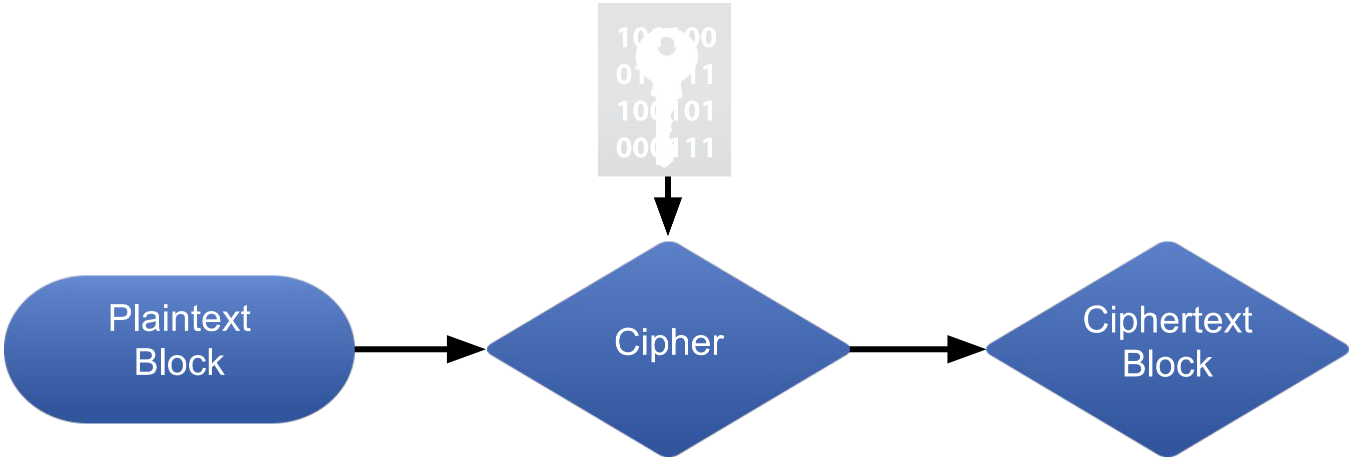


Block and Stream Ciphers

Stream Cipher



Block Cipher



What is Cryptography?

“Cryptography is the science of using mathematics to encrypt and decrypt data.”

- Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.
- Cryptanalysis is the science of analyzing and breaking secure communication.
- Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck.

What is Cryptography?

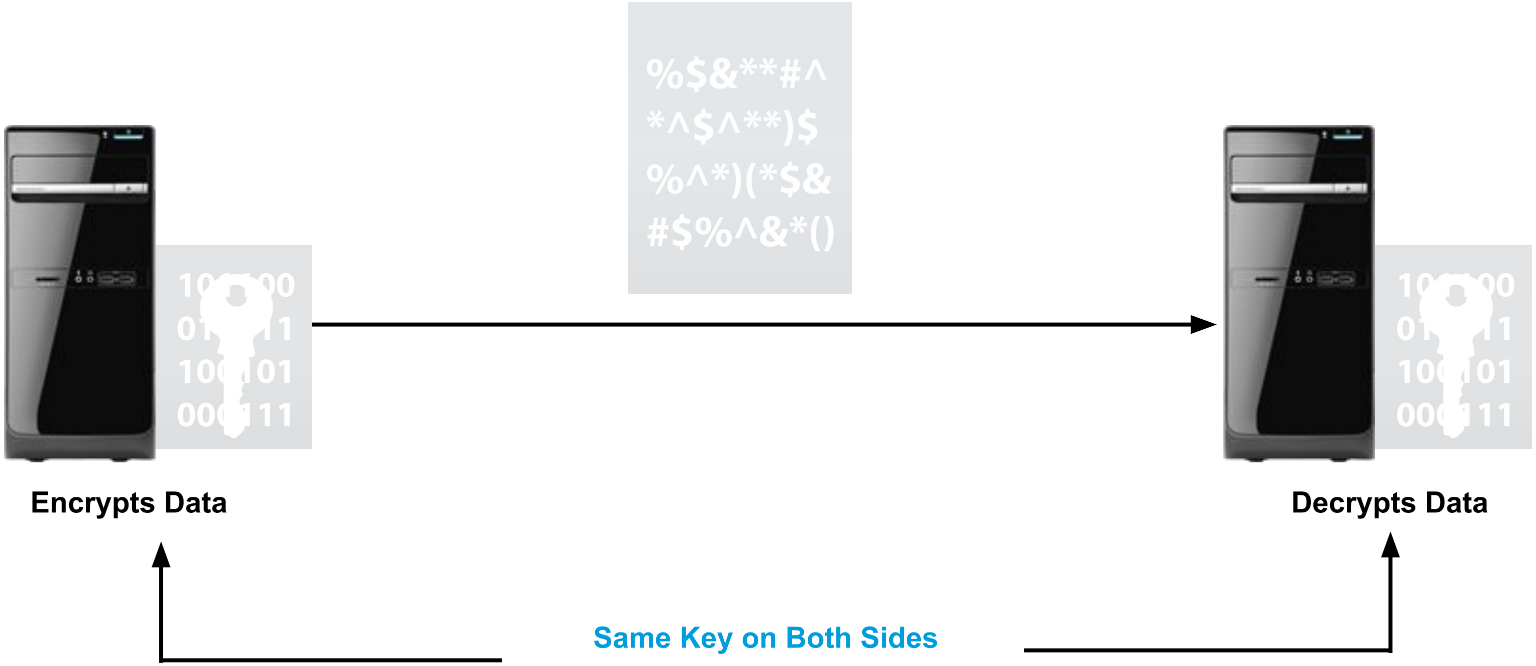
- Cryptography can be strong or weak.
- Cryptographic strength is measured in the time and resources it would require to recover the plaintext.
- The result of strong cryptography is ciphertext that is very difficult to decipher without possession of the appropriate decoding tool.
- How difficult?
  - Given all of today's computing power and available time — even a billion computers doing a billion checks a second — it is not possible to decipher the result of strong cryptography before the end of the universe.

How does Cryptography work?

- A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process.
- A cryptographic algorithm works in combination with a key — a word, number, or phrase — to encrypt the plaintext.
- The same plaintext encrypts to different ciphertext with different keys.
- The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.
- A cryptographic algorithm, plus all possible keys and all the protocols that make it work make up a cryptosystem.

Symmetric Cryptography

- In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption.
- The Advanced Encryption Standard (AES) is an example of a modern conventional cryptosystem.



Encrypts Data

Decrypts Data

Same Key on Both Sides

Symmetric Cryptography

- Conventional encryption has benefits.
  - It is very fast.
  - It is especially useful for encrypting data that is not going anywhere.
- Expensive - due to the difficulty of secure key distribution.
- Sender and recipient must agree upon a key and keep it secret between themselves.
- If they are in different physical locations, they must trust a courier or some other secure communication medium to prevent the disclosure of the secret key during transmission.

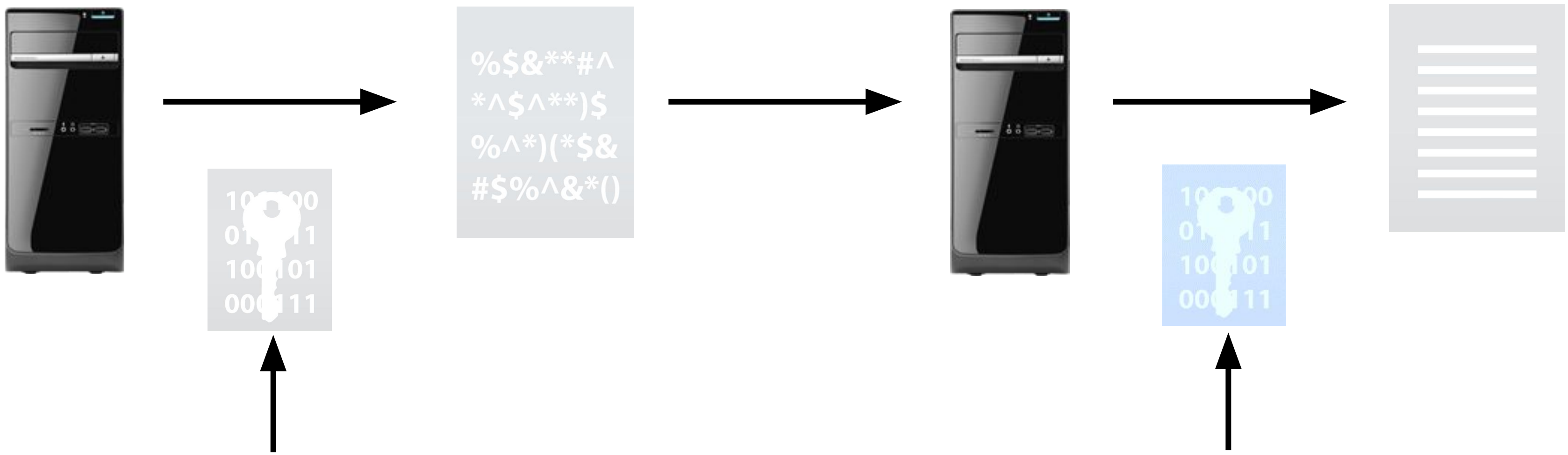
Symmetric Cryptography

- Anyone who overhears or intercepts the key in transit can later read, modify, and forge all information encrypted or authenticated with that key.
- The persistent problem with conventional encryption is key distribution: how do you get the key to the recipient without someone intercepting it?
- Symmetric Systems use:
  - Data Encryptions Standard (DES)
  - 3DES
  - AES
  - Blowfish
  - Twofish
  - RC 4, 5, 6

Asymmetric Cryptography

- The problems of key distribution are solved by public key cryptography, the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1975.
- Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption.
- You publish your public key to the world while keeping your private key secret.
- Anyone with a copy of your public key can then encrypt information that only you can read. Even people you have never met.

Asymmetric Cryptography



Public Key Encrypts

Private Key Decrypts

Asymmetric Cryptography

- Only the person who has the corresponding private key can decrypt the information.
- It is computationally infeasible to deduce the private key from the public key.
- The primary benefit of public key cryptography is that it allows people who have no pre-existing security arrangement to exchange messages securely.
- The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared.

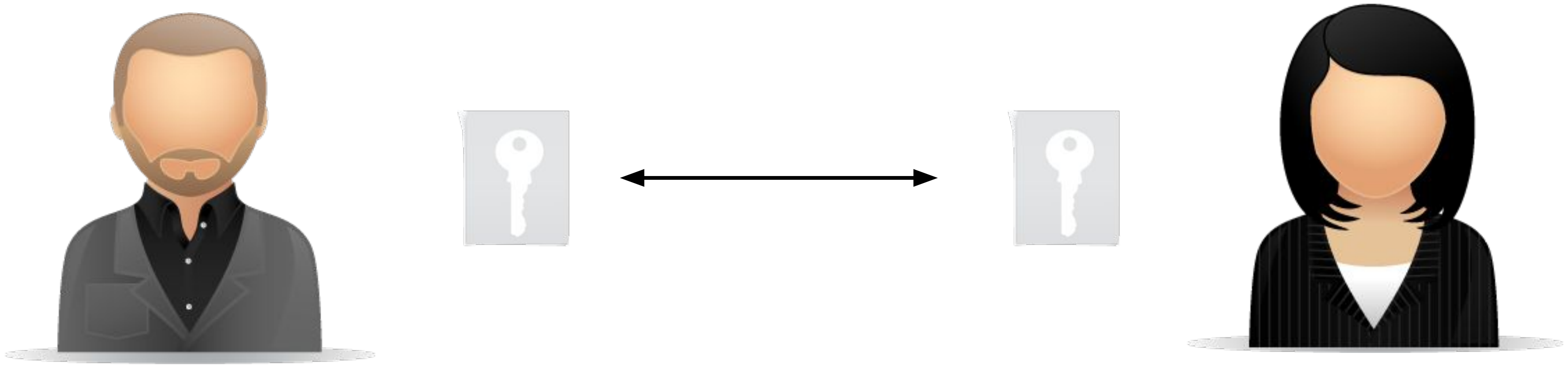
Asymmetric Cryptography

- Some examples of public-key cryptosystems are:
  - Elgamal (named for its inventor, Taher Elgamal)
  - RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman)
  - Diffie-Hellman (named for its inventors)
  - DSA, the Digital Signature Algorithm (invented by David Kravitz).
- Public key encryption was the technological revolution that provides strong cryptography to the adult masses.

Keys

- A key is a value that works with a cryptographic algorithm to produce a specific ciphertext.
- Keys are basically really big numbers.
- Key size is measured in bits; the number representing a 1024-bit key is quite large.
- In public key cryptography, the bigger the key, the more secure the ciphertext.
- However, public key size and conventional cryptography's secret key size are totally unrelated.
  - A conventional 128-bit key is equivalent to a 3000-bit public key. Again, the bigger the key, the more secure, but the algorithms used for each type of cryptography are very different.

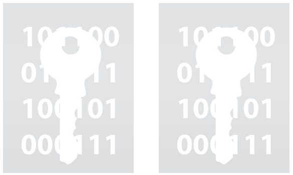
Key Exchange



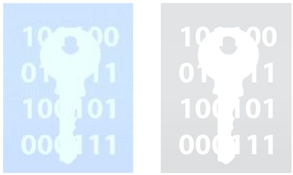
Sender

Receiver

For messages to be exchanged, the sender and receiver need the right cryptographic keys



Symmetric cipher:
Same key



Asymmetric cipher:
Each other’s public key

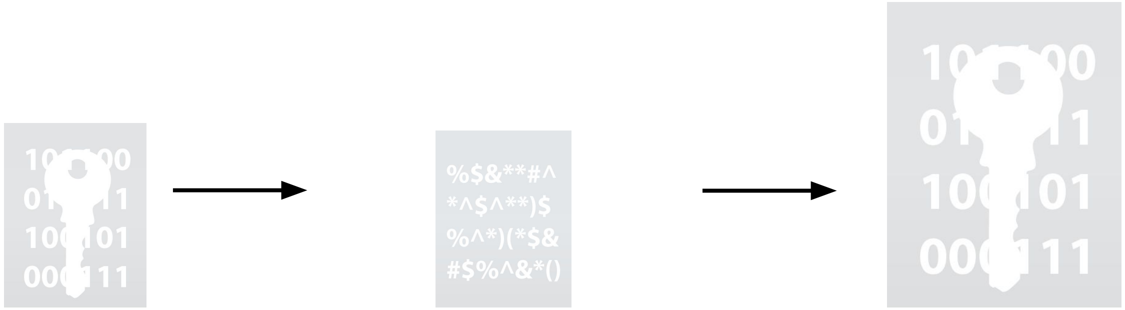
Keys

- While the public and private keys are mathematically related, it's very difficult to derive the private key given only the public key; however, deriving the private key is possible given enough time and computing power.
- This makes it very important to pick keys of the right size; large enough to be secure, but small enough to be applied fairly quickly.
- Additionally, you need to consider who might be trying to read your files, how determined they are, how much time they have, and what their resources might be.

Keys

- Larger keys will be cryptographically secure for a longer period of time.
- If what you want to encrypt needs to be hidden for many years, you might want to use a very large key.
- Note: Keys are stored in encrypted form.

Key Stretching



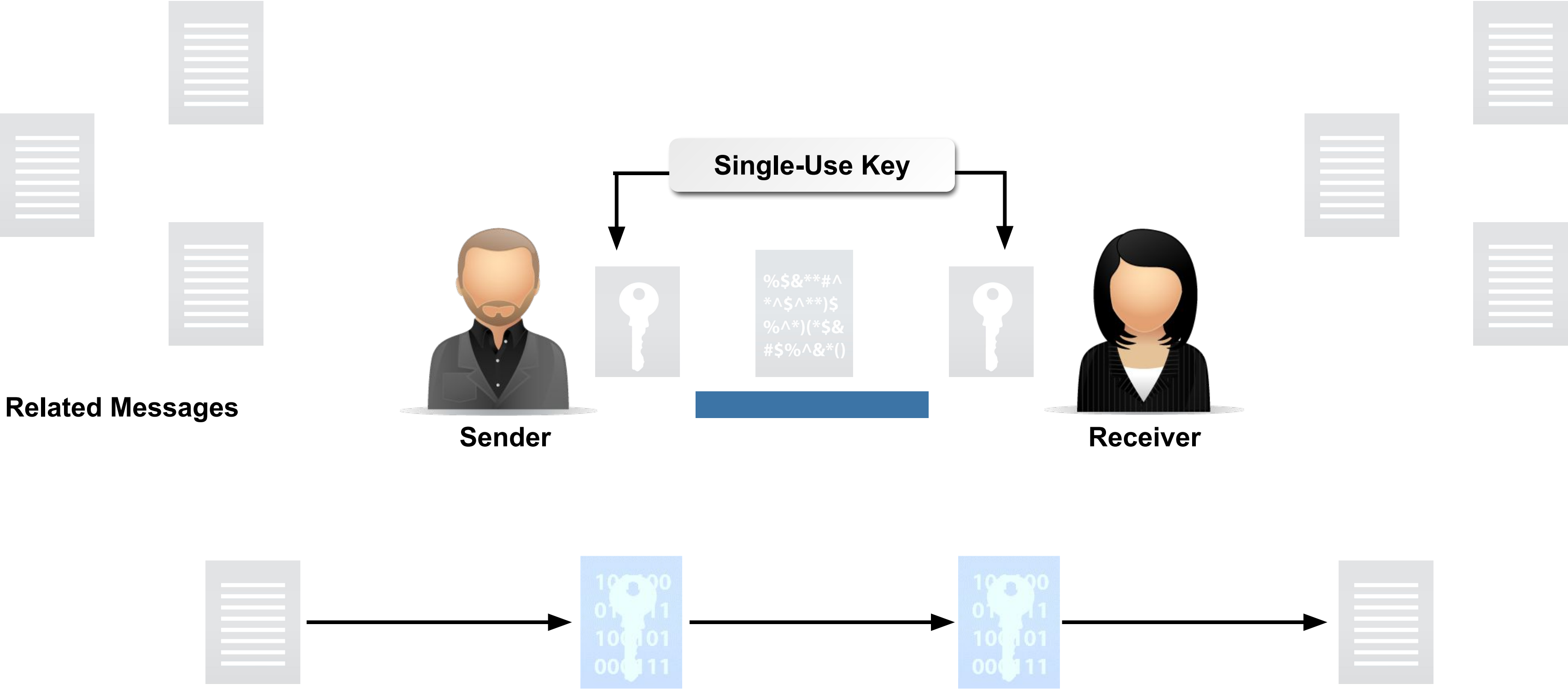
Original Key

Key Stretching Algorithm

Enhanced Key

Key stretching makes it harder to crack passwords and passphrases.

Session Keys



Single-Use Key

Related Messages

Sender

Receiver

Unrelated message requires a different key

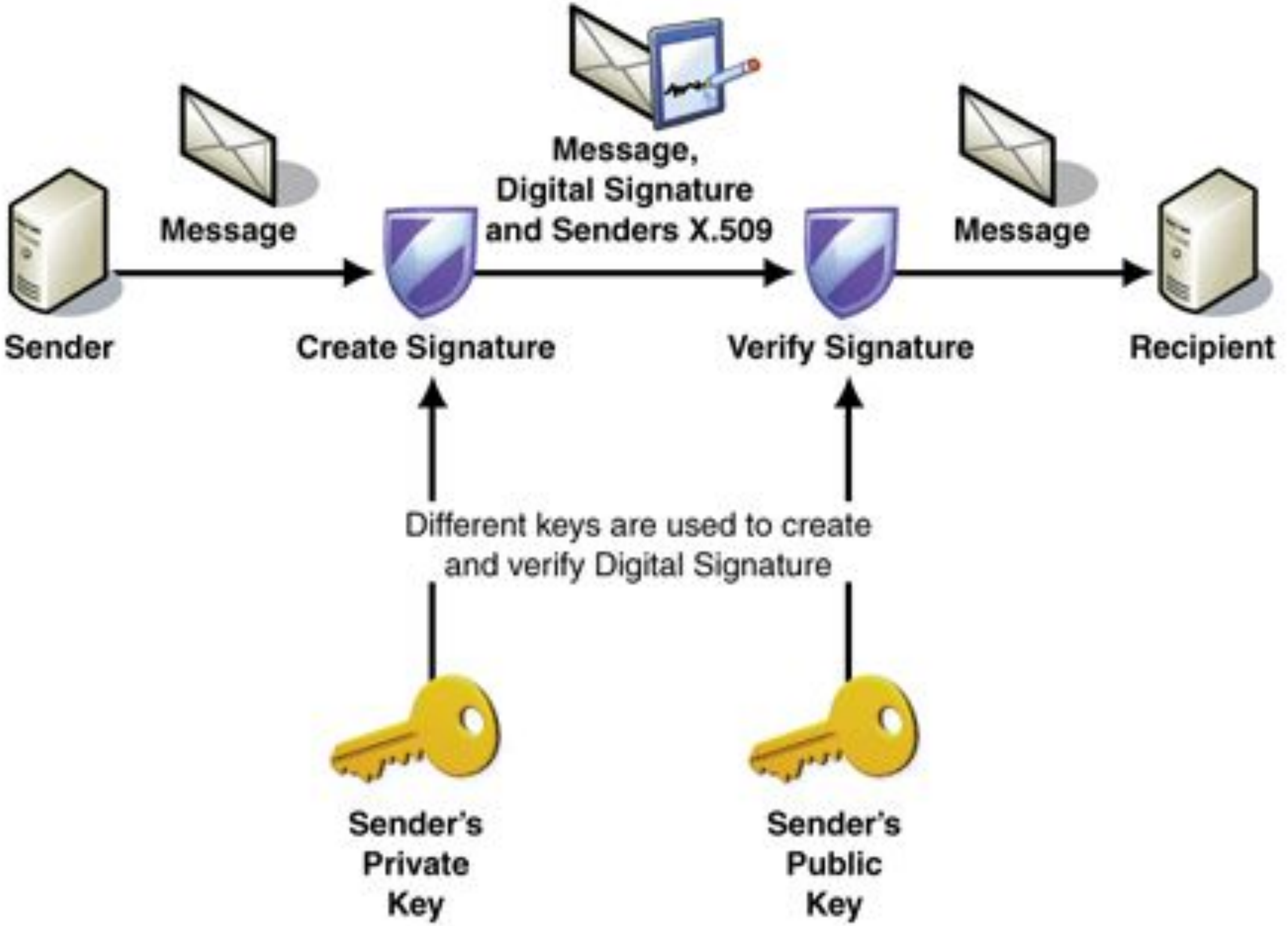
Digital Signatures

- A major benefit of public key cryptography is that it provides a method for employing digital signatures.
- Digital signatures enable the recipient of information to verify the authenticity of the information's origin, and also verify that the information is intact.
- Public key digital signatures provide authentication and data integrity.
- A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information.
- These features are every bit as fundamental to cryptography as privacy.

Digital Signatures

- A digital signature serves the same purpose as a handwritten signature.
- A digital signature attests to the contents of the information as well as to the identity of the signer.
- You sign information with your private key. If the information can be verified with your public key, then it must have originated with you.

Digital Signatures



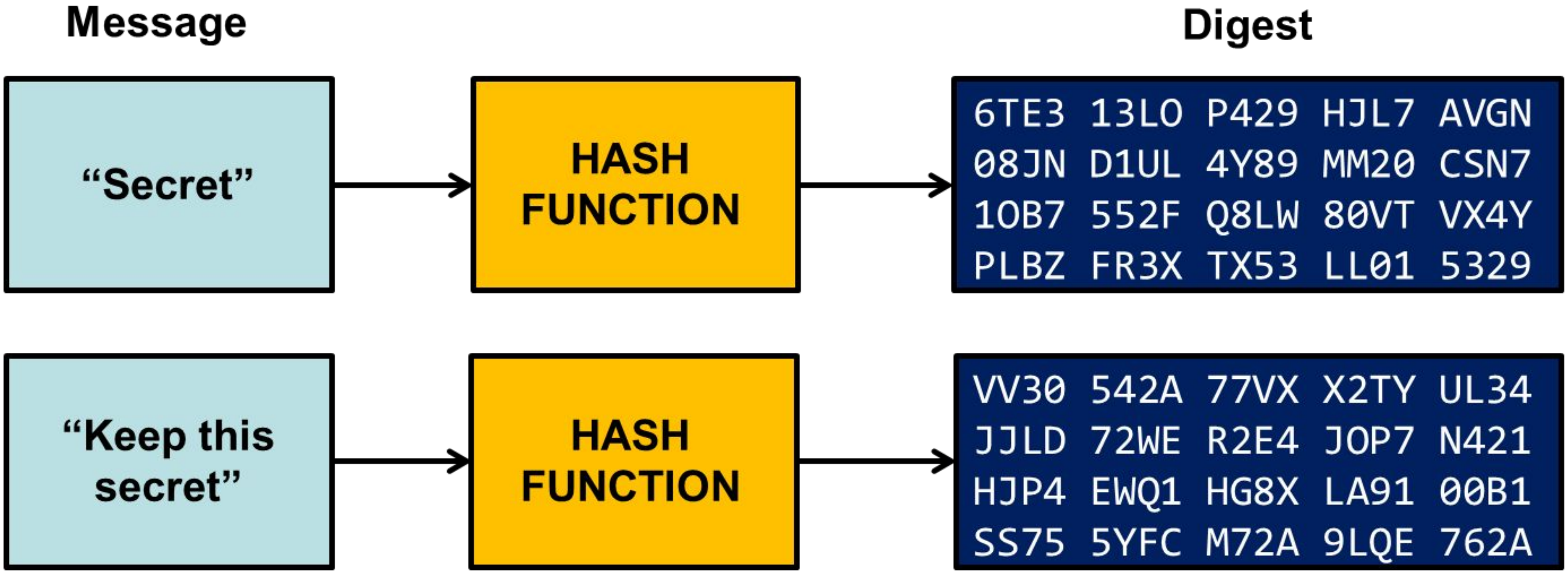
Hash Functions

- Digital Signatures have some problems.
  - They can be slow and produce an enormous volume of data — at least double the size of the original information.
- An improvement on this is the addition of a one-way hash function in the process.
- A one-way hash function takes variable-length input — in this case, a message of any length, even thousands or millions of bits — and produces a fixed-length output, known as the message digest; say, 160-bits.
- The hash function ensures that, if the information is changed, an entirely different output value is produced.

Hash Functions

- As long as a secure hash function is used, there is no way to take someone's signature from one document and attach it to another, or to alter a signed message in any way.
- The slightest change in a signed document will cause the digital signature verification process to fail.

Hash Functions



Message

Digest

“Secret” → HASH FUNCTION →

```
6TE3 13LO P429 HJL7 AVGN
08JN D1UL 4Y89 MM20 CSN7
1OB7 552F Q8LW 80VT VX4Y
PLBZ FR3X TX53 LL01 5329
```

“Keep this secret” → HASH FUNCTION →

```
VV30 542A 77VX X2TY UL34
JJLD 72WE R2E4 JOP7 N421
HJP4 EWQ1 HG8X LA91 00B1
SS75 5YFC M72A 9LQE 762A
```

Digital Certificates

- One issue with public key cryptosystems is that users must be constantly vigilant to ensure that they are encrypting to the correct person's key.
- In an environment where it is safe to freely exchange keys via public servers, man-in-the-middle attacks are a potential threat.
- In this type of attack, someone posts a phony key with the name and user ID of the user's intended recipient. Data encrypted to — and intercepted by — the true owner of this bogus key is now in the wrong hands.

Digital Certificates

- In a public key environment, it is vital that you are assured that the public key to which you are encrypting data is in fact the public key of the intended recipient and not a forgery.
- You could simply encrypt only to those keys which have been physically handed to you.
- But suppose you need to exchange information with people you have never met; how can you tell that you have the correct key?
- Digital certificates simplify the task of establishing whether a public key truly belongs to the alleged owner.

Digital Certificates

- A certificate is a form of credential.
- Example: Driver's license or your birth certificate.
  - Each of these has some information on it identifying you and some authorization stating that someone else has confirmed your identity. Some certificates, such as your passport, are important enough confirmation of your identity that you would not want to lose them
- A digital certificate is information included with a person's public key that helps others verify that a key is genuine or valid.
- Digital certificates are used to thwart attempts to substitute one person's key for another.

Digital Certificates

- A digital certificate consists of three things:
    - A public key.
    - Certificate information. ("Identity" information about the user, such as name, user ID, and so on.)
    - One or more digital signatures.
- The purpose of the digital signature on a certificate is to state that the certificate information has been attested to by some other person or entity.
- The digital signature does not attest to the authenticity of the certificate as a whole; it vouches only that the signed identity information goes along with, or is bound to, the public key.

Digital Certificates

- Thus, a certificate is basically a public key with one or two forms of ID attached, plus a stamp of approval from some other trusted individual.

Digital Certificates – Certificate Distribution

- Certificates are used when it's necessary to exchange public keys with someone else.
- For small groups of people who wish to communicate securely, it is easy to manually exchange USB Keys or emails containing each owner's public key.
- This is manual public key distribution, and it is practical only to a certain point.
- Beyond that point, it is necessary to put systems into place that can provide the necessary security, storage, and exchange mechanisms so coworkers, business partners, or strangers could communicate if need be.

Digital Certificates – Certificate Distribution

- These can come in the form of storage-only repositories called Certificate Servers, or more structured systems that provide additional key management features and are called Public Key Infrastructures (PKIs).
- Certificate servers
  - A certificate server, also called a key server, is a database that allows users to submit and retrieve digital certificates.
  - A certificate server usually provides some administrative features that enable a company to maintain its security policies — for example, allowing only those keys that meet certain requirements to be stored.

Public Key Infrastructures

- Public Key Infrastructure
  - A PKI contains the certificate storage facilities of a certificate server, but also provides certificate management facilities (the ability to issue, revoke, store, retrieve, and trust certificates).
  - The main feature of a PKI is the introduction of what is known as a Certification Authority, or CA
    - which is a human entity — a person, group, department, company, or other association — that an organization has authorized to issue certificates to its computer users. (A CA's role is similar to a country's government Passport Office.)

Public Key Infrastructures

- A CA creates certificates and digitally signs them using the CA's private key.
- Because of its role in creating certificates, the CA is the central component of a PKI.
- Using the CA's public key, anyone wanting to verify a certificate's authenticity verifies the issuing CA's digital signature, and so, the integrity of the contents of the certificate (most importantly, the public key and the identity of the certificate holder).

Certificate Revocation

- Certificates are only useful while they are valid.
- It is unsafe to simply assume that a certificate is valid forever.
- In most organizations and in all PKIs, certificates have a restricted lifetime. This constrains the period in which a system is vulnerable should a certificate compromise occur.
- Certificates are created with a scheduled validity period: a start date/time and an expiration date/ time.

Certificate Revocation

- There are situations where it is necessary to invalidate a certificate prior to its expiration date, such as when an the certificate holder terminates employment with the company or suspects that the certificate's corresponding private key has been compromised.
- This is called revocation. A revoked certificate is much more suspect than an expired certificate.
- Anyone who has signed a certificate can revoke his or her signature on the certificate (provided he or she uses the same private key that created the signature).

Certificate Revocation

- When a certificate is revoked, it is important to make potential users of the certificate aware that it is no longer valid.
- In a PKI environment, communication of revoked certificates is most commonly achieved via a data structure called a Certificate Revocation List, or CRL, which is published by the CA.
- The CA distributes the CRL to users at some regularly scheduled interval (and potentially off-cycle, whenever a certificate is revoked).

What is Pretty Good Privacy (PGP)?

- "It's personal. It's private. And it's no one's business but yours. You may be planning a political campaign, discussing your taxes, or having a secret romance. Or you may be communicating with a political dissident in a repressive country. Whatever it is, you don't want your private electronic mail (email) or confidential documents read by anyone else. There's nothing wrong with asserting your privacy. Privacy is as apple-pie as the Constitution."
  - Phil Zimmermann

PGP Symmetric Algorithms

- PGP (Pretty Good Privacy) offers a selection of different secret key algorithms to encrypt actual plain-text messages.
- The three symmetric block ciphers offered by PGP are:
  - CAST,
  - Triple-DES, and
  - IDEA.
- The reasoning behind this was that they were 3 highly secure cryptographic algorithms.

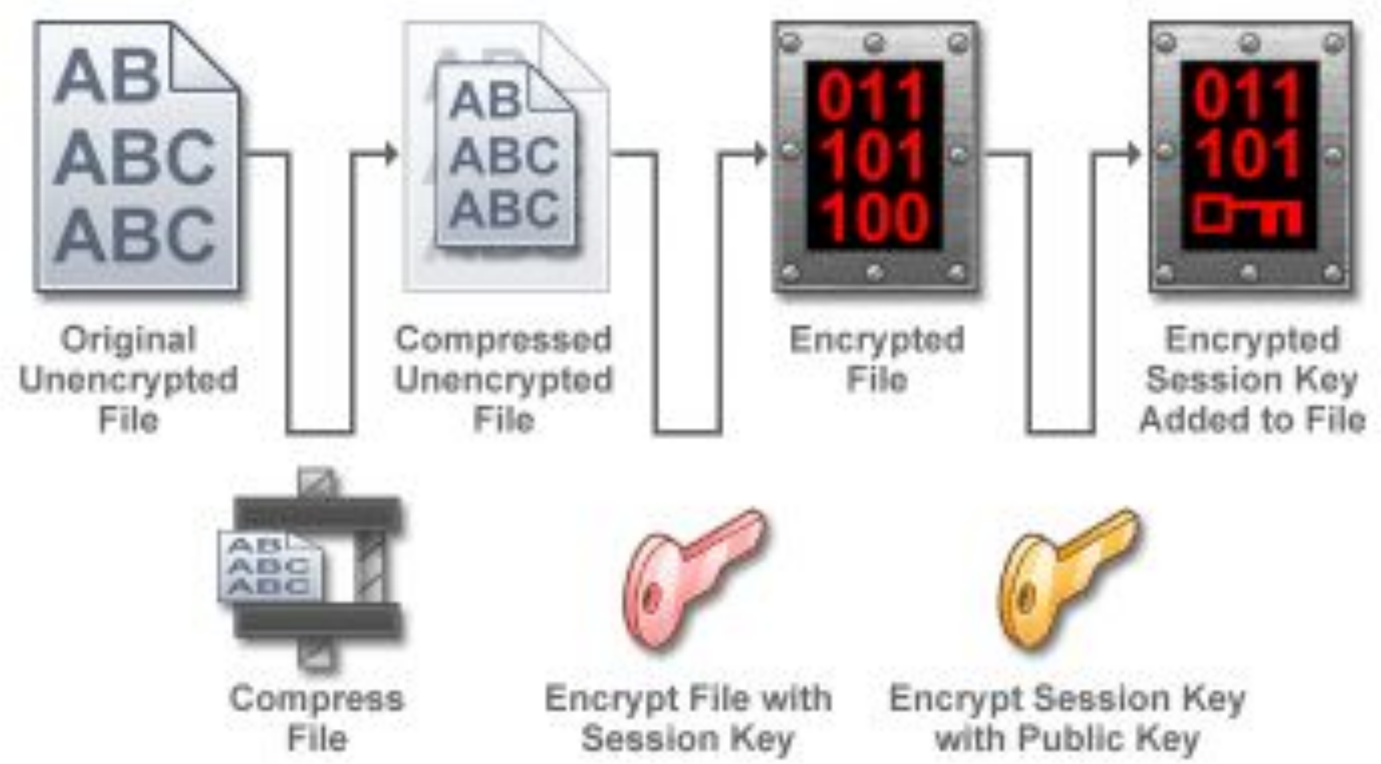
How PGP Works – Encryption

- PGP combines some of the best features of both conventional and public key cryptography.
- PGP is a hybrid cryptosystem.
- When a user encrypts plaintext with PGP, PGP first compresses the plaintext.
    - Data compression saves modem transmission time and disk space and, more importantly, strengthens cryptographic security.
    - Most cryptanalysis techniques exploit patterns found in the plaintext to crack the cipher.
    - Compression reduces these patterns in the plaintext, thereby greatly enhancing resistance to cryptanalysis.

How PGP Works – Encryption

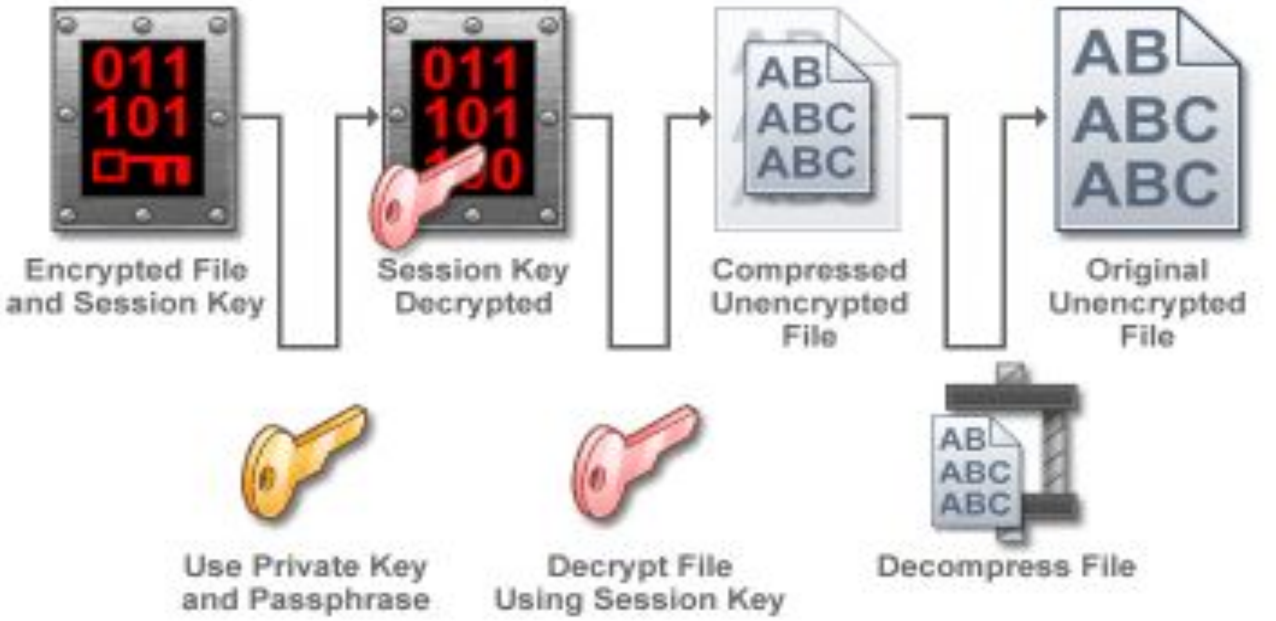
- PGP then creates a session key, which is a one-time-only secret key.
- This key is a random number generated from the random movements of your mouse and the keystrokes you type.
- This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext.
- Once the data is encrypted, the session key is then encrypted to the recipient's public key.
- This public key-encrypted session key is transmitted along with the ciphertext to the recipient.

How PGP Works – Encryption


AB
ABC
ABC
Original Unencrypted File
AB
ABC
ABC
Compressed Unencrypted File
011
101
100
Encrypted File
011
101
Encrypted Session Key Added to File
AB
ABC
ABC
Compress File
Encrypt File with Session Key
Encrypt Session Key with Public Key

How PGP Works - Decryption

- Decryption works in the reverse. The recipient's copy of PGP uses his or her private key to recover the temporary session key, which PGP then uses to decrypt the conventionally-encrypted ciphertext.



How PGP Works - Keys

- Keys are stored in encrypted form.
- PGP stores the keys in two files on your hard disk; one for public keys and one for private keys. These files are called keyrings.
- As you use PGP, you will typically add the public keys of your recipients to your public keyring.
- Combines the convenience of the key distribution of public key encryption with the speed of conventional encryption.

How PGP Signing Works

- PGP uses a cryptographically strong hash function on the plaintext the user is signing.
- This generates a fixed-length data item known as a message digest.
- Then PGP uses the digest and the private key to create the "signature"
- PGP transmits the signature and the plaintext together.
- Upon receipt of the message, the recipient uses PGP to recompute the digest, thus verifying the signature.

How PGP Works – PGP Certificates

- One unique aspect of the PGP certificate format is that a single certificate can contain multiple signatures.
- Several or many people may sign the key/ identification pair to attest to their own assurance that the public key definitely belongs to the specified owner.
- PGP certificates fully support a hierarchical structure using a CA to validate certificates.

Validity & Trust

- PGP uses digital signatures as its form of introduction.
- When any user signs another's key, he or she becomes an introducer of that key. As this process goes on, it establishes a web of trust.
- In a PGP environment, any user can act as a CA.
- Any PGP user can validate another PGP user's public key certificate.
- You indicate, on your copy of my key, whether you think my judgment counts. It's really a reputation system: certain people are reputed to give good signatures, and people trust them to attest to other keys' validity.