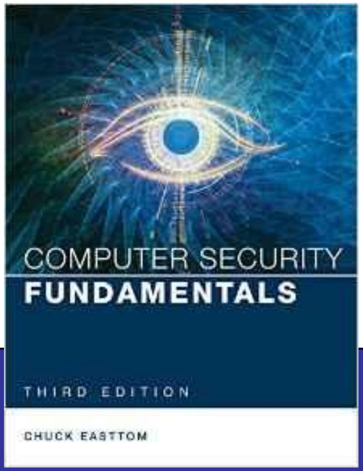
Computer Security Fundamentals

by Chuck Easttom



Chapter 8 Encryption

Chapter 8 Objectives

- Explain the basics of encryption
- Discuss modern cryptography methods
- Select appropriate cryptography for your organization
- Understand the function and protocols of VPNs

- **Encryption**

Encryption, as name suggests, is generally a technique that is used to conceal message using algorithms. It is fundamental application of cryptography that encodes a message with an algorithm. In generally helps to protect private information, sensitive data, and enhance security of communication among client apps and servers. It is considered one of most effective and popular data security techniques.

- **Cryptography**

Cryptography, as name suggests, is generally study of methods like encryption. Its main objective is to provide methods simply to secure and protect information and communications using encryption and related techniques. It simply allows one to store sensitive information or transmit it across insecure networks so that it cannot be read or accessed by anyone except intended recipient. Its functions include authentication, nonrepudiation, confidentiality and integrity.

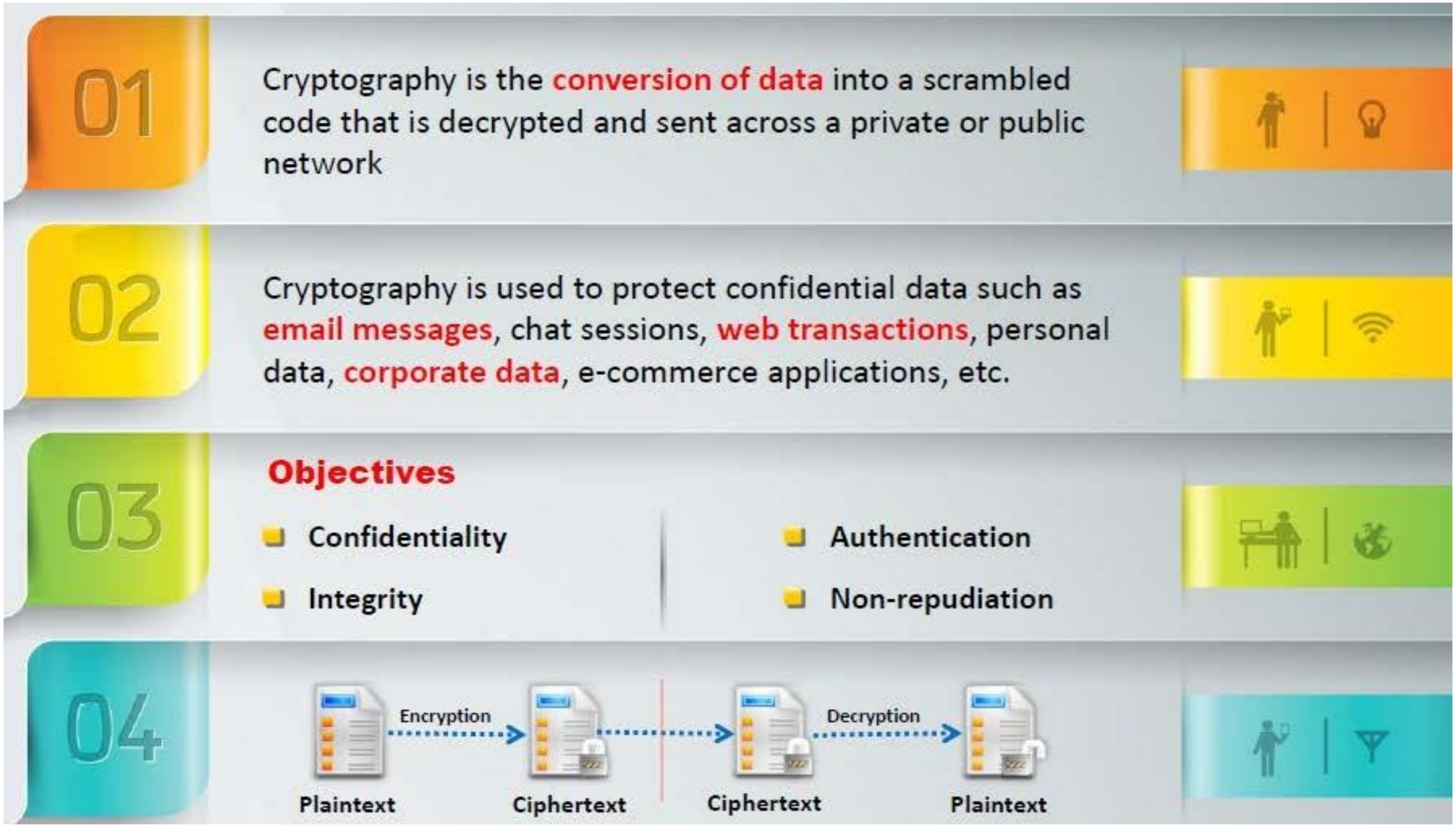
Introduction

- Encryption
  - Scrambling information.
  - One critical part to the security puzzle.
  - Without it, all security measures are inadequate.
- Cryptography
  - An art form

Cryptography Basics

- Decryption
  - Reversal of the scrambling protocol
- Encryption
  - Algorithm scrambles plain
  - Sender and receiver agree on algorithm
  - Message difficult to re-create without protocol

Cryptography?



01

Cryptography is the **conversion of data** into a scrambled code that is decrypted and sent across a private or public network

02

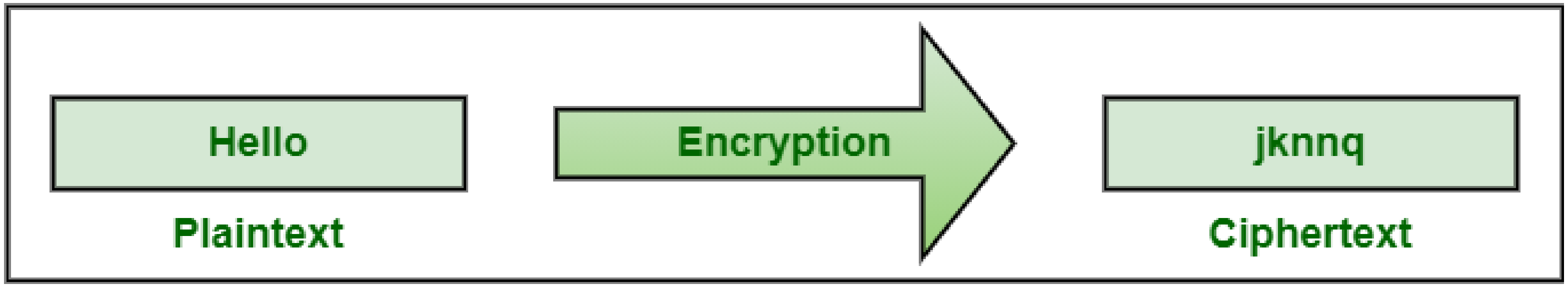
Cryptography is used to protect confidential data such as **email messages**, chat sessions, **web transactions**, personal data, **corporate data**, e-commerce applications, etc.

03

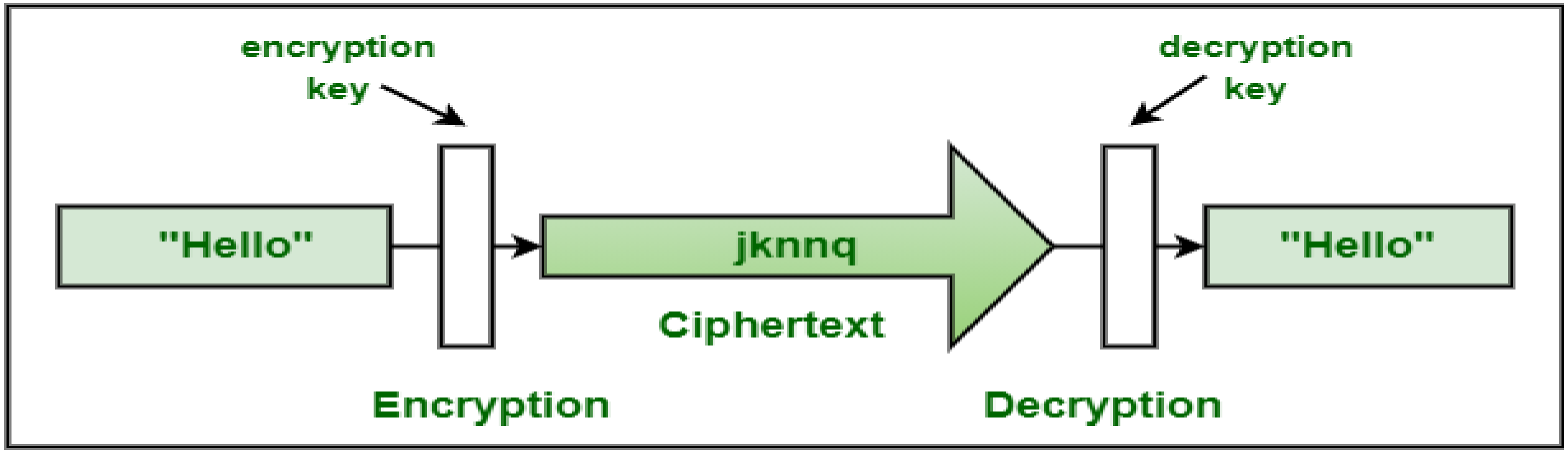
Objectives

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

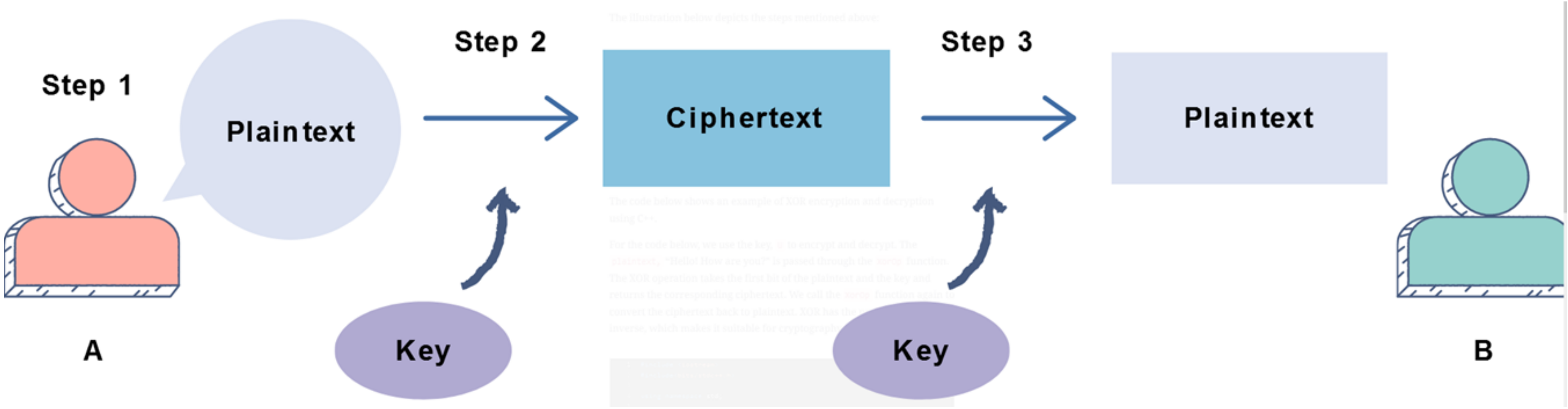
04



Encryption

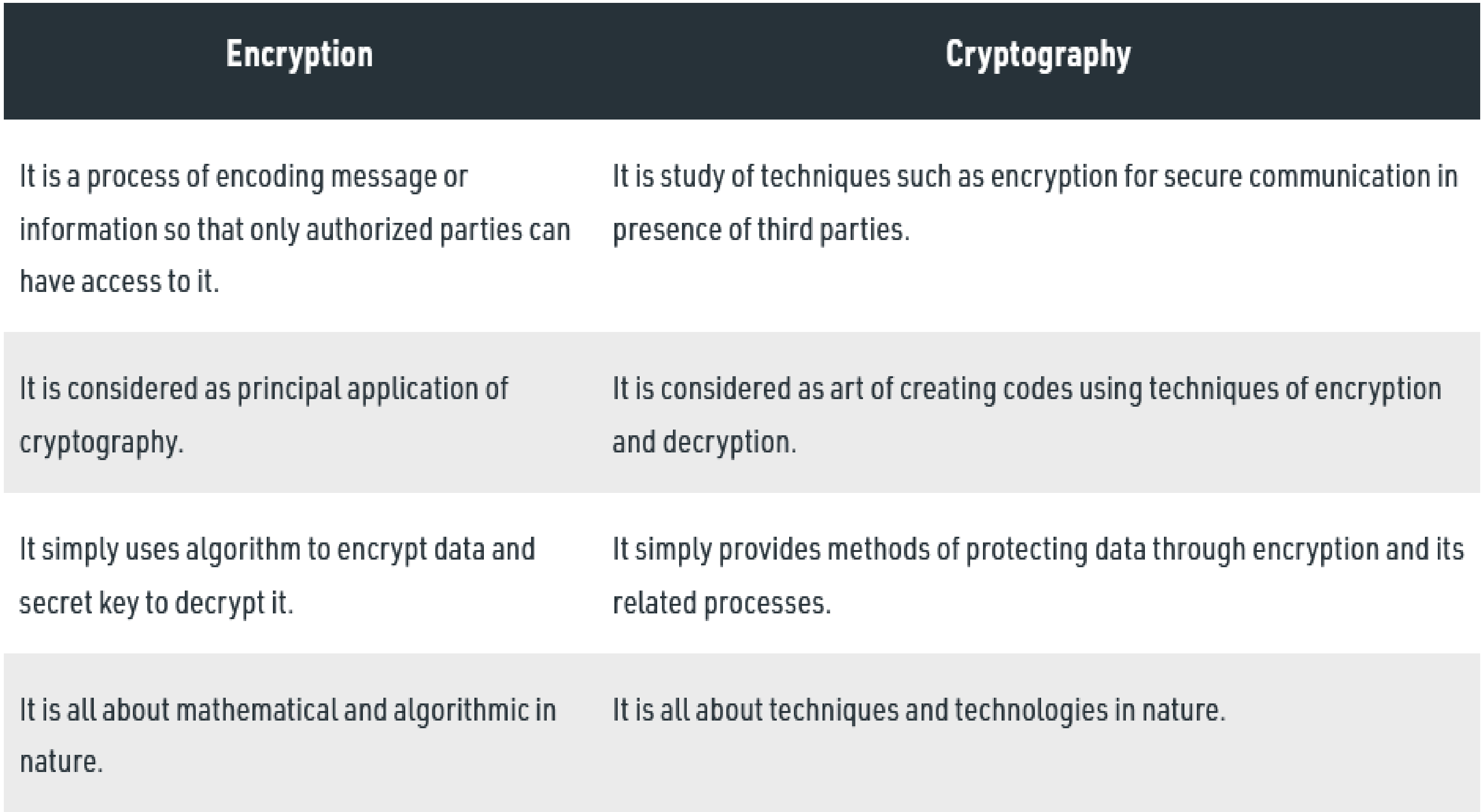


Cryptography



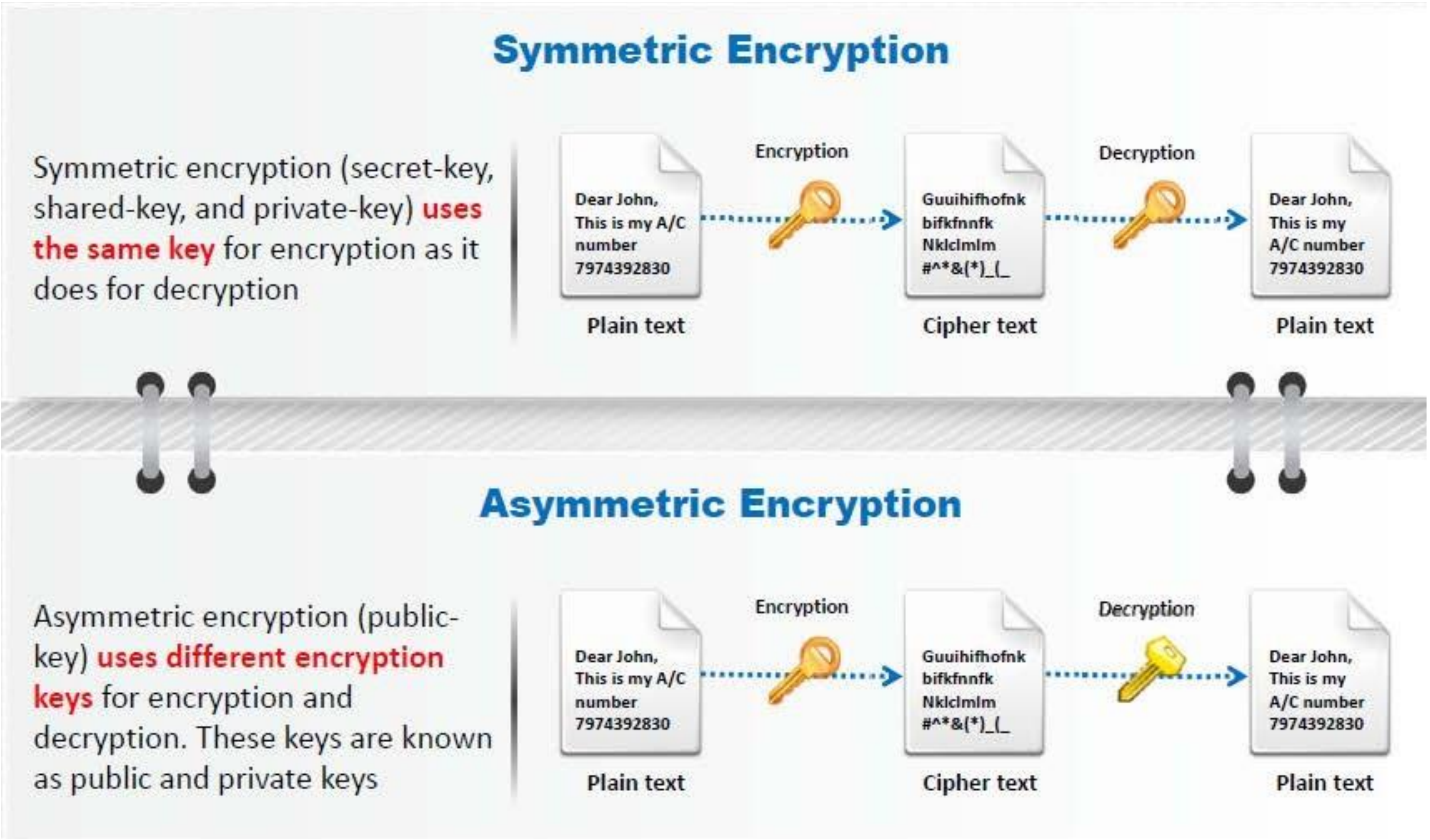
Step 1
Plaintext
A
Step 2
Key
Ciphertext
Step 3
Key
Plaintext
B

Difference between Encryption and Cryptography



Encryption	Cryptography
It is a process of encoding message or information so that only authorized parties can have access to it.	It is study of techniques such as encryption for secure communication in presence of third parties.
It is considered as principal application of cryptography.	It is considered as art of creating codes using techniques of encryption and decryption.
It simply uses algorithm to encrypt data and secret key to decrypt it.	It simply provides methods of protecting data through encryption and its related processes.
It is all about mathematical and algorithmic in nature.	It is all about techniques and technologies in nature.

Types of Cryptography



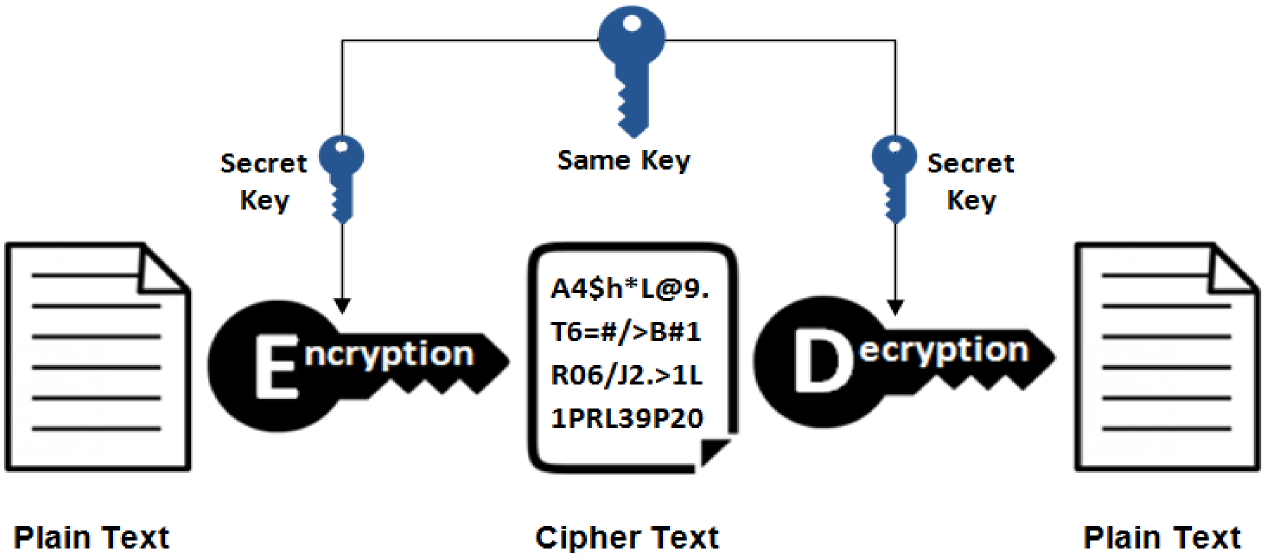
Symmetric Encryption

Symmetric encryption (secret-key, shared-key, and private-key) **uses the same key** for encryption as it does for decryption

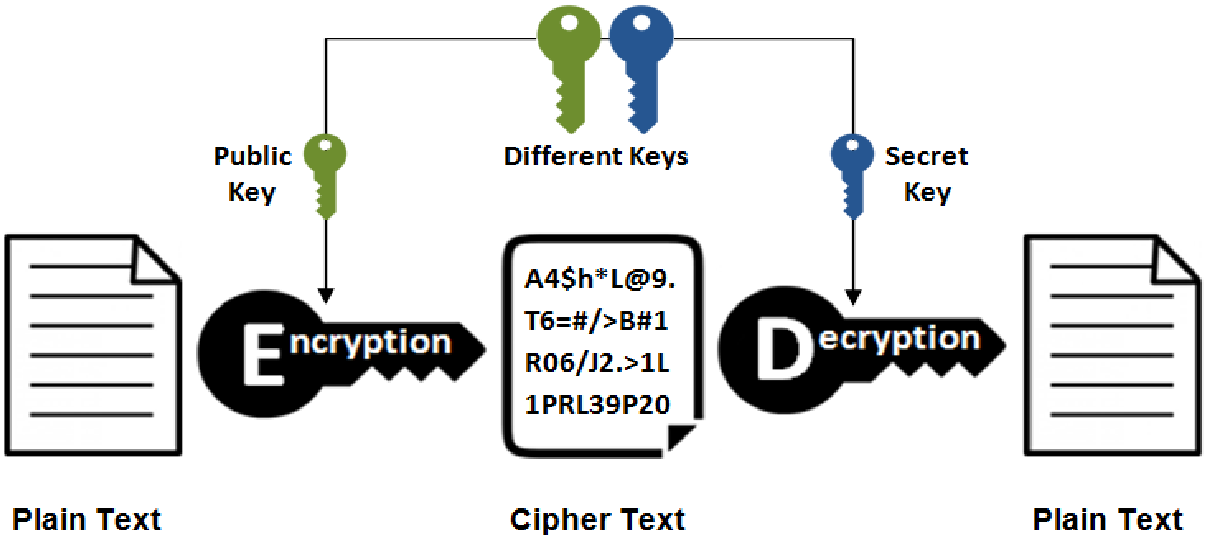
Asymmetric Encryption

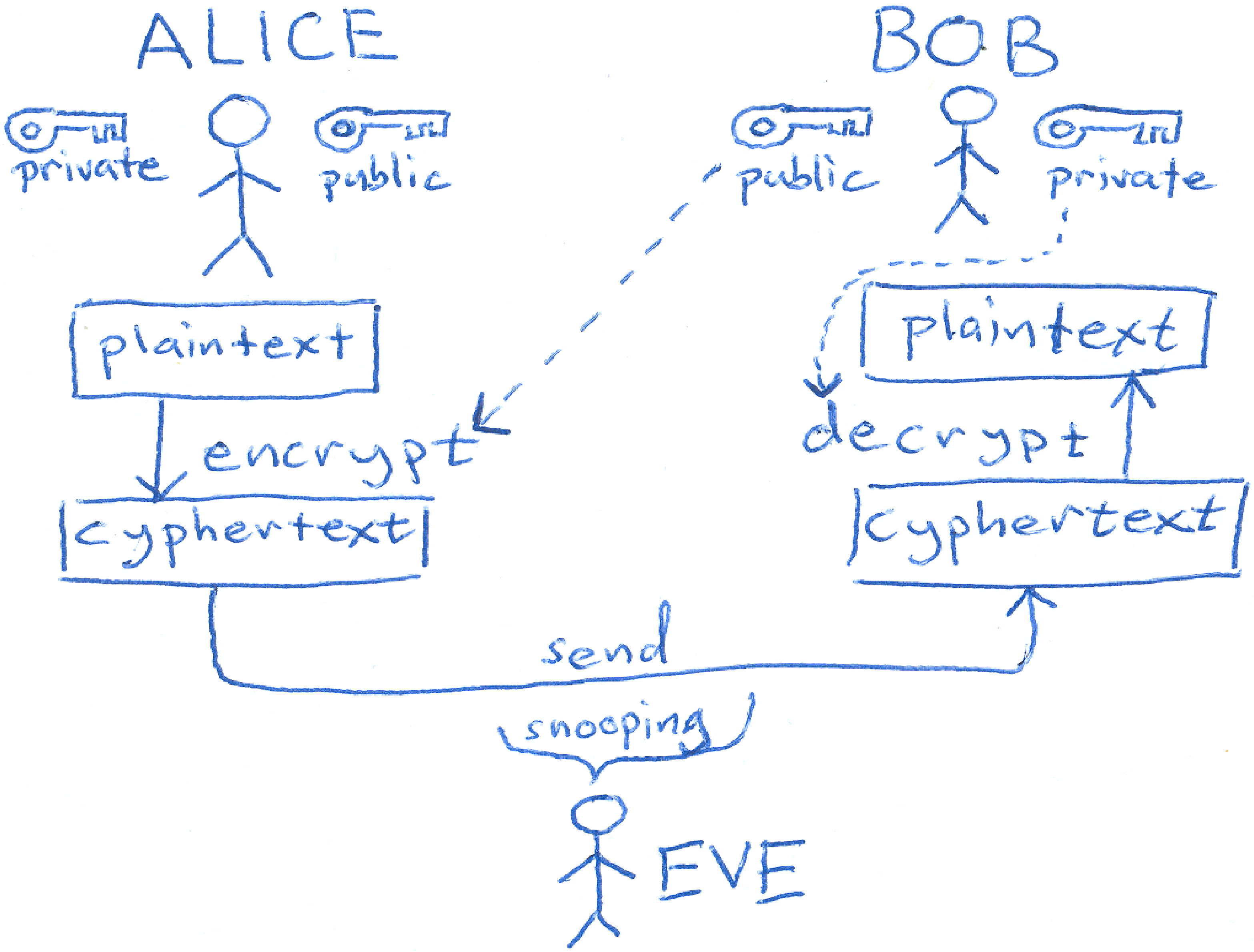
Asymmetric encryption (public-key) **uses different encryption keys** for encryption and decryption. These keys are known as public and private keys

Symmetric Encryption



Asymmetric Encryption

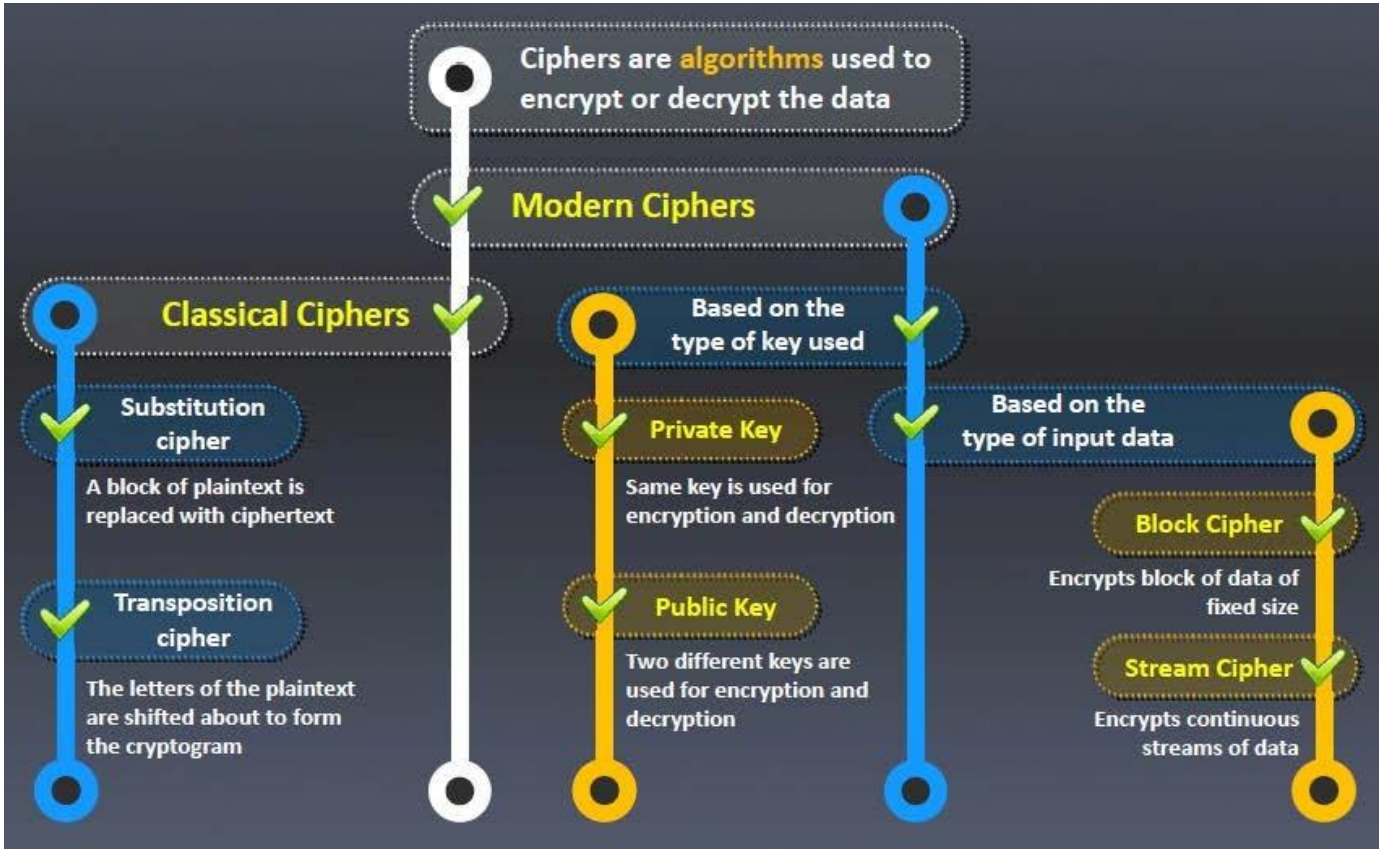



ALICE
private
public
plaintext
encrypt
cyphertext
BOB
public
private
plaintext
decrypt
cyphertext
send
snooping
EVE

Types of Cryptography (cont.)

- Single/symmetric key encryption
  - Stream
  - Block
    - Substitution and transposition
- Public/asymmetric key encryption

Ciphers



Ciphers are algorithms used to encrypt or decrypt the data

Modern Ciphers

Classical Ciphers

Substitution cipher

A block of plaintext is replaced with ciphertext

Transposition cipher

The letters of the plaintext are shifted about to form the cryptogram

Based on the type of key used

Private Key

Same key is used for encryption and decryption

Public Key

Two different keys are used for encryption and decryption

Based on the type of input data

Block Cipher

Encrypts block of data of fixed size

Stream Cipher

Encrypts continuous streams of data

History of Encryption

- Old as written communication and war
- Caesar Cipher
  - Shift cipher
    - A DOG
      - Shift 1 – B EPH
      - Shift 2 – C FQI
      - Shift negative 1 – Z CNF

History of Encryption (cont.)

- Caesar Cipher
  - Frequency distribution cracks this simple cipher.
  - Substitution alphabet.
    - Substitutes one letter in the alphabet for another.

History of Encryption (cont.)

- Multi-alphabetic
  - Select multiple shifts
    - Shift 1, 2, –1
    - Rotate through the shifts
    - A DOG becomes B FNH
  - Old cipher considered weak today

Binary Operations

- Binary Operations
  - AND, OR, XOR

- Example of AND operation

$$\begin{array}{cccc} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 \end{array}$$

Binary Operations

- Example of OR operation

$$\begin{array}{cccc} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ \hline 1 & 1 & 0 & 1 \end{array}$$

Binary Operations

- Example of XOR operation

$$\begin{array}{cccc} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 0 & 0 \end{array}$$

Binary Operations

- XOR only reversible binary operation
  - Convert plain text to ASCII

    A DOG = 065 032 068 079 071

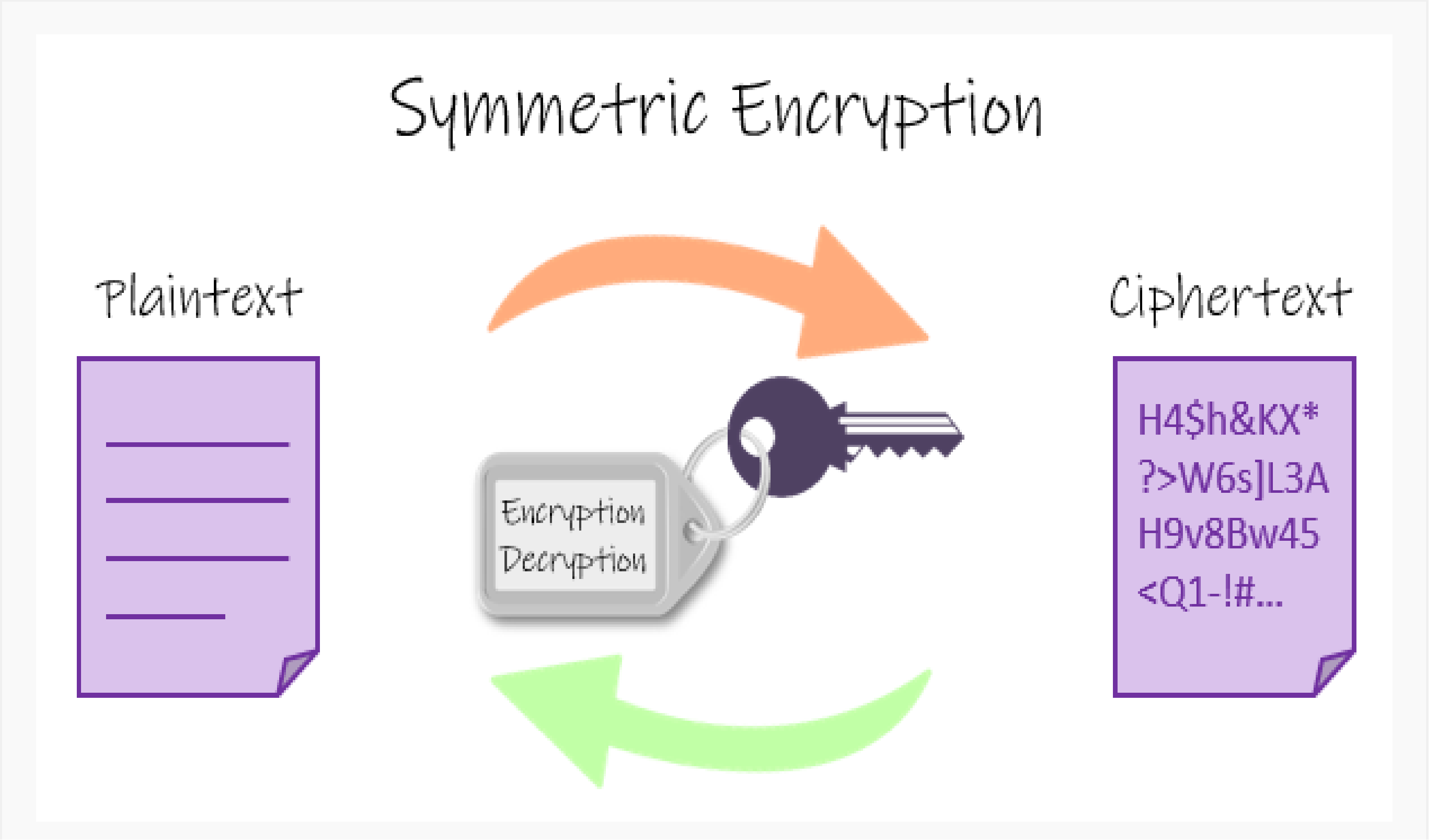
  - Then, convert ASCII to binary

    0100 0001, 0100 0100, 0100 1111, 0100 0111

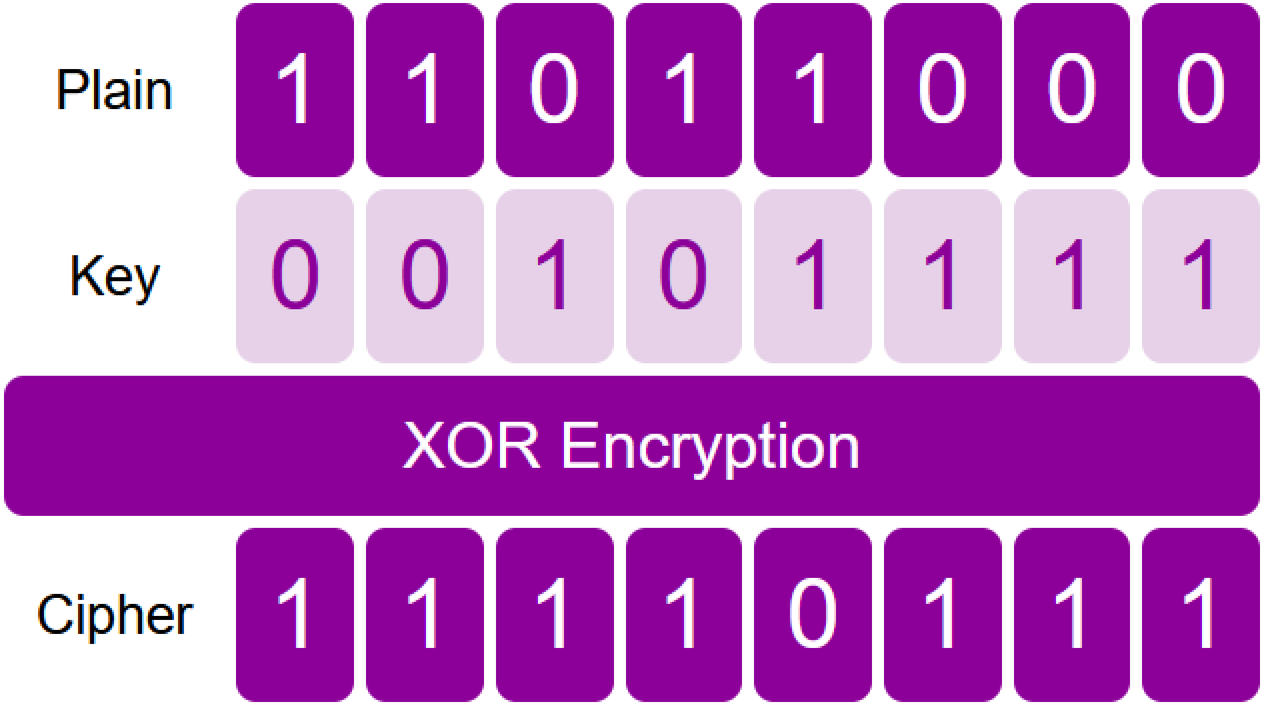
Cryptography Terms

- Key: The bits that are combined with the plain text to encrypt it. In some cases this is random numbers; in other cases it is the result of some mathematical operation.
- Plain text: The unencrypted text.
- Cipher text: The encrypted text.
- Algorithm: A mathematical process for doing something.

XOR Encryption Algorithm

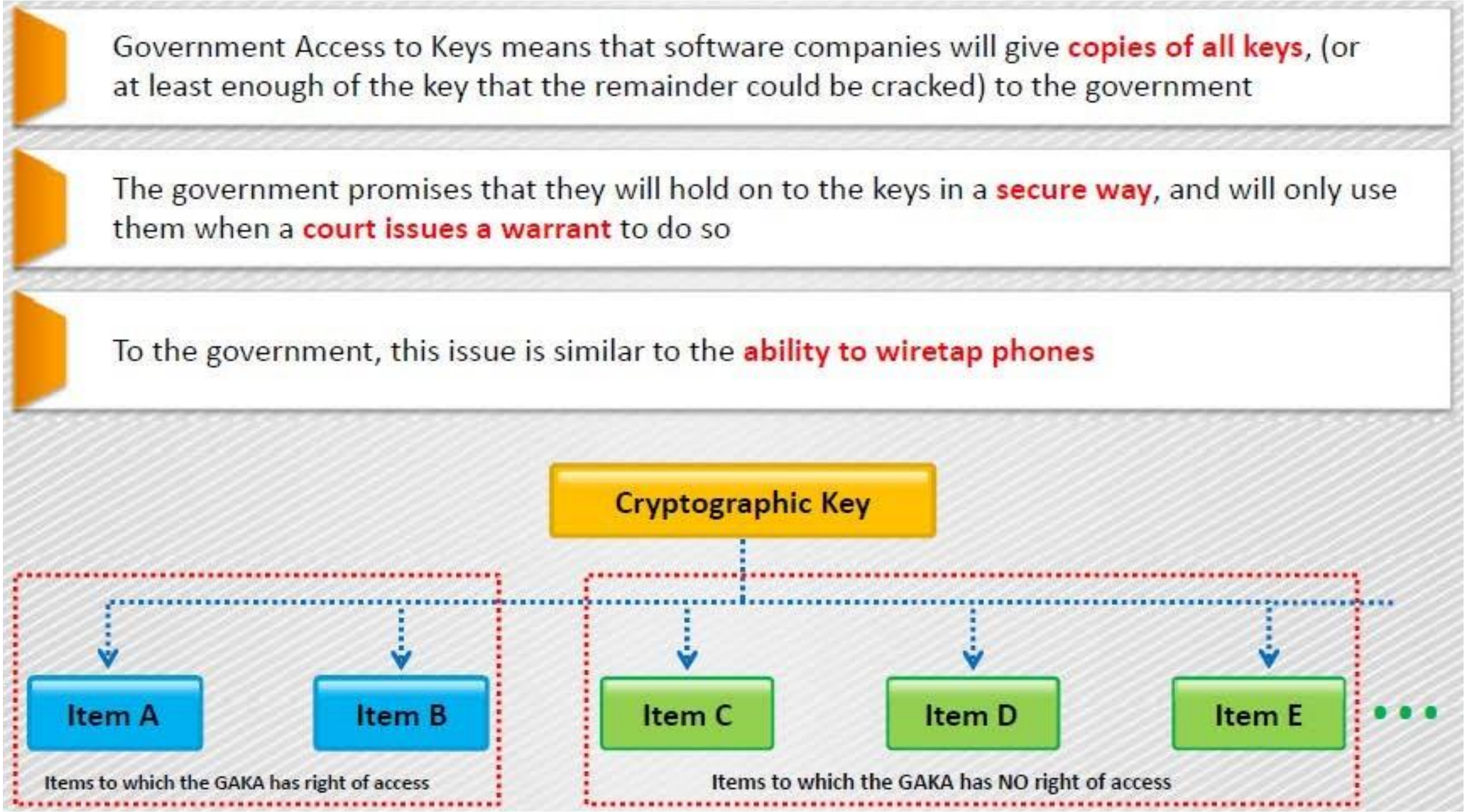


XOR Encryption Algorithm



Plain	1	1	0	1	1	0	0	0
Key	0	0	1	0	1	1	1	1
XOR Encryption								
Cipher	1	1	1	1	0	1	1	1

Government Access to Keys (GAK)



- Government Access to Keys means that software companies will give **copies of all keys**, (or at least enough of the key that the remainder could be cracked) to the government
- The government promises that they will hold on to the keys in a **secure way**, and will only use them when a **court issues a warrant** to do so
- To the government, this issue is similar to the **ability to wiretap phones**

Cryptographic Key

Item A

Item B

Items to which the GAKA has right of access

Item C

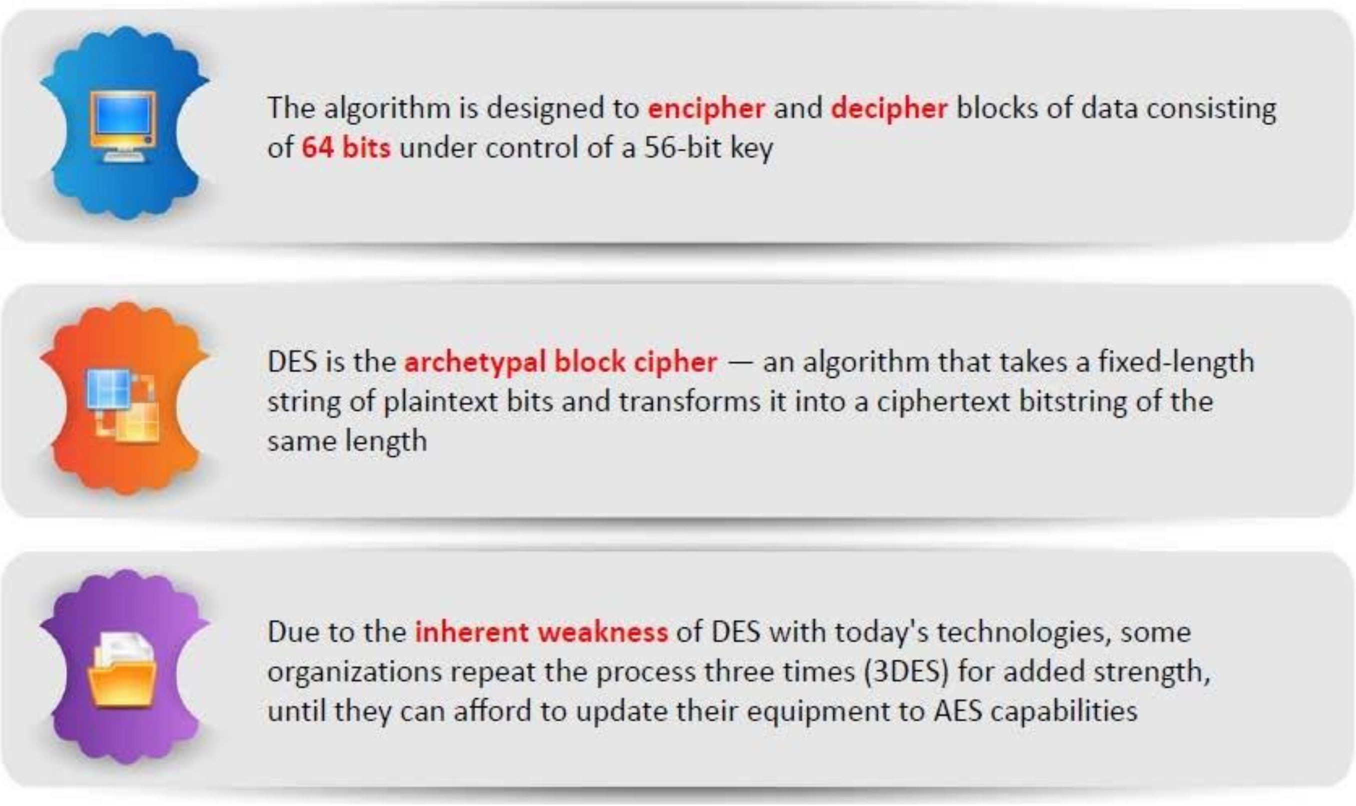
Item D

Item E

• • •

Items to which the GAKA has NO right of access

Modern Methods…Data Encryption Standard (DES)

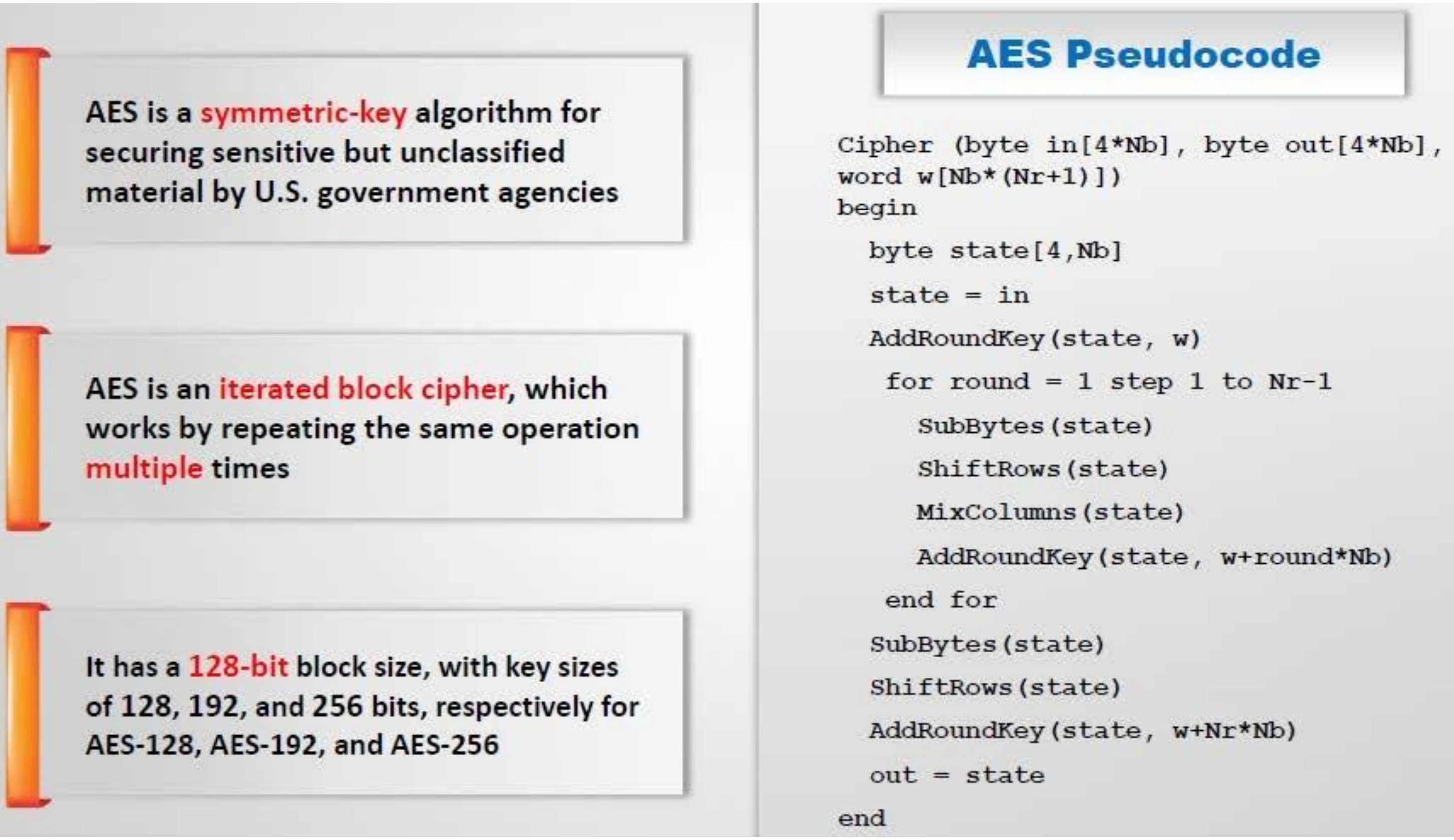


The algorithm is designed to **encipher** and **decipher** blocks of data consisting of **64 bits** under control of a 56-bit key

DES is the **archetypal block cipher** — an algorithm that takes a fixed-length string of plaintext bits and transforms it into a ciphertext bitstring of the same length

Due to the **inherent weakness** of DES with today's technologies, some organizations repeat the process three times (3DES) for added strength, until they can afford to update their equipment to AES capabilities

Advanced Encryption Standard (AES)



AES is a symmetric-key algorithm for securing sensitive but unclassified material by U.S. government agencies

AES is an iterated block cipher, which works by repeating the same operation multiple times

It has a 128-bit block size, with key sizes of 128, 192, and 256 bits, respectively for AES-128, AES-192, and AES-256

AES Pseudocode

```
Cipher (byte in[4*Nb], byte out[4*Nb],
word w[Nb*(Nr+1)])
begin
  byte state[4,Nb]
  state = in
  AddRoundKey(state, w)
   for round = 1 step 1 to Nr-1
     SubBytes(state)
     ShiftRows(state)
     MixColumns(state)
     AddRoundKey(state, w+round*Nb)
   end for
  SubBytes(state)
  ShiftRows(state)
  AddRoundKey(state, w+Nr*Nb)
  out = state
end
```

Modern Methods (cont.)

- Data Encryption Standard (DES)

1. Divided into 64-bit blocks; then transposed

2. Manipulated by 16 steps of encryption, using 56-bit key

3. Scrambled by a swapping algorithm

4. Transposed one final time

Modern Methods (cont.)

- Advanced Encryption Standard (AES).
- Advanced Encryption Standard was the algorithm eventually chosen to replace DES. It is a block cipher that works on 128-bit blocks. It can have one of three key sizes of 128, 192, or 256 bits. This was selected by the United States government to be the replacement for DES and is now the most widely used symmetric key algorithm.

Modern Methods (cont.)

- One major problem with symmetric key encryption

  How do you transmit the symmetric key?

- The answer: public key encryption

Modern Methods (cont.)

- Public key (asymmetric) encryption
  - Opposite of single key encryption.
  - One key (public key) used to encrypt .
  - One key (private key) used to decrypt.
  - Only holder of a private key can decrypt messages.

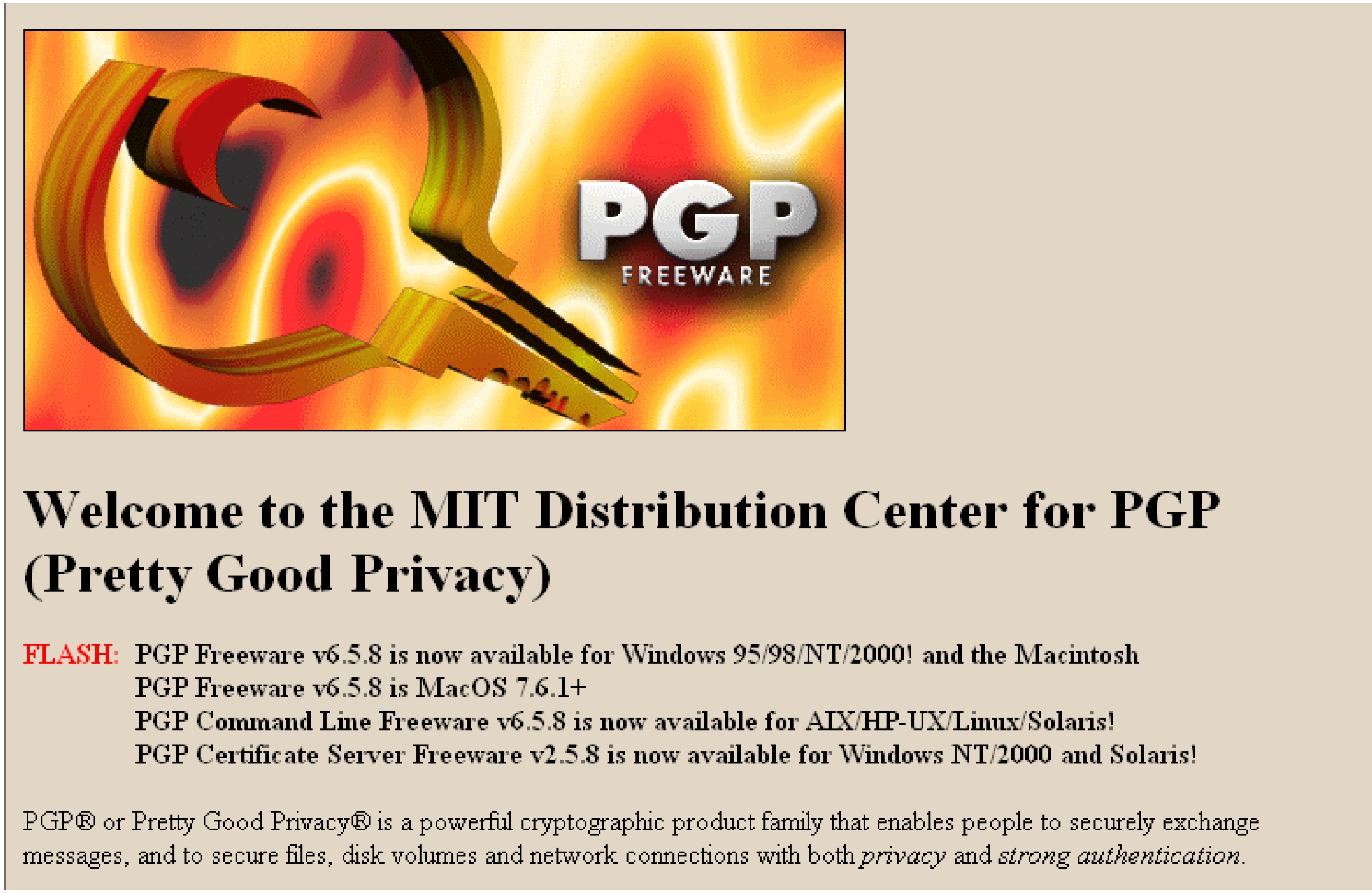
Modern Methods (cont.)

- Public key (asymmetric) encryption
  - Public key encryption is most widely used.
  - Pretty Good Privacy (PGP):
    - Freeware
    - Quite secure

Modern Methods (cont.)

- Public key (asymmetric) encryption
  - Pretty Good Privacy (PGP)
    - Freeware
    - Phil Zimmerman – 2004
    - Quite secure

Modern Methods (cont.)



Welcome to the MIT Distribution Center for PGP (Pretty Good Privacy)

FLASH: PGP Freeware v6.5.8 is now available for Windows 95/98/NT/2000! and the Macintosh
PGP Freeware v6.5.8 is MacOS 7.6.1+
PGP Command Line Freeware v6.5.8 is now available for AIX/HP-UX/Linux/Solaris!
PGP Certificate Server Freeware v2.5.8 is now available for Windows NT/2000 and Solaris!

PGP® or Pretty Good Privacy® is a powerful cryptographic product family that enables people to securely exchange messages, and to secure files, disk volumes and network connections with both *privacy* and *strong authentication*.

The MIT Distribution Center for PGP home page
(http://web.mit.edu/network/pgp.html)

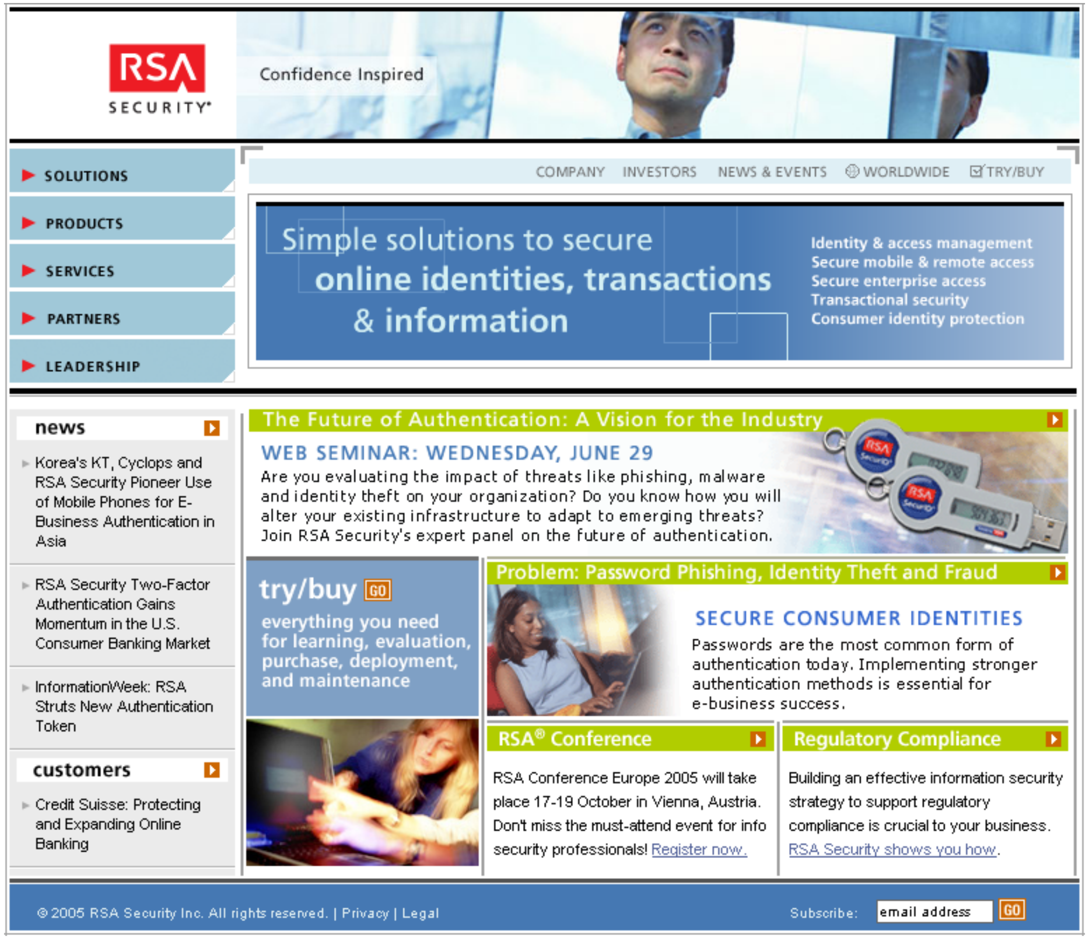
Modern Methods (cont.)

- Public key (asymmetric) encryption
  - RSA
    - You start by generating two large random primes, p and q, of approximately equal size. Now you need to pick two numbers so that when multiplied together the product will be the size you want (that is, 128 bits, 256 bits, and so on).
    - Now multiply p and q to get n.
    - Let n = pq
    - Let m = (p - 1)(q – 1)

Modern Methods (cont.)

- Public key (asymmetric) encryption
  - RSA
    - Now select another number; call this number e. Pick e so that it is co-prime to m.
    - Choose a small number e, co-prime to m.
    - Youare almost done generating a key. Now you just find a number d that when multiplied by e and modulo m would yield a 1. (Note: Modulo means to divide two numbers and return the remainder. For example 8 modulo 3 would be 2.).
    - Find d, such that de % m = 1.
    - Now publish e and n as the public key. Keep d and n as the secret key. To encrypt, simply take your message raised to the e power and modulo n.

Modern Methods (cont.)



RSA SECURITY

Confidence Inspired

Simple solutions to secure online identities, transactions & information

- Identity & access management
- Secure mobile & remote access
- Secure enterprise access
- Transactional security
- Consumer identity protection

news

- Korea's KT, Cyclops and RSA Security Pioneer Use of Mobile Phones for E-Business Authentication in Asia
- RSA Security Two-Factor Authentication Gains Momentum in the U.S. Consumer Banking Market
- InformationWeek: RSA Struts New Authentication Token

customers

- Credit Suisse: Protecting and Expanding Online Banking

The Future of Authentication: A Vision for the Industry

WEB SEMINAR: WEDNESDAY, JUNE 29

Are you evaluating the impact of threats like phishing, malware and identity theft on your organization? Do you know how you will alter your existing infrastructure to adapt to emerging threats? Join RSA Security's expert panel on the future of authentication.

try/buy GO

everything you need for learning, evaluation, purchase, deployment, and maintenance

Problem: Password Phishing, Identity Theft and Fraud

SECURE CONSUMER IDENTITIES

Passwords are the most common form of authentication today. Implementing stronger authentication methods is essential for e-business success.

RSA® Conference

RSA Conference Europe 2005 will take place 17-19 October in Vienna, Austria. Don't miss the must-attend event for info security professionals! Register now.

Regulatory Compliance

Building an effective information security strategy to support regulatory compliance is crucial to your business. RSA Security shows you how.

© 2005 RSA Security Inc. All rights reserved. | Privacy | Legal

Subscribe: email address GO

The RSA Security home page
(http://www.rsasecurity.com)

Modern Methods (cont.)

- Legitimate versus fraudulent encryption
  - Warning signs of frauds
    - Unbreakable
    - Certified
    - Inexperienced people

Avoid ‘bad’ crypto

- Unbreakable
- Unhackable
- Secret algorithm
- Kerhoff’s principle
- This can be formally expressed as Kerckhoff’s principle. Auguste Kerckhoff first articulated this in the 1800s, stating that the security of a cipher depends only on the secrecy of the key, not the secrecy of the algorithm.

Encryptions used in Internet

- Symmetric algorithms are faster, and require a shorter key length to be as secure as asymmetric algorithms. However, there is the problem of how to securely exchange keys. So most e-commerce solutions use an asymmetric algorithm to exchange symmetric keys and then use the symmetric keys to encrypt the actual data.

Digital Signatures

- A digital signature is not used to ensure the confidentiality of a message, but rather to guarantee who sent the message. This is referred to as nonrepudiation. Essentially, it proves who the sender is. Digital signatures are actually rather simple, but clever. They simply reverse the asymmetric encryption process. Recall that in asymmetric encryption the public key (which anyone can have access to) is used to encrypt a message to the recipient, and the private key (which is kept secure and private) can decrypt it. With a digital signature, the sender encrypts something with his private key. If the recipient can decrypt that with the sender's public key, then it must have been sent by the person purported to have sent the message.

Hash

- Hashing is a type of cryptographic algorithm that has some specific characteristics. First and foremost it is one way. That means you cannot "unhash" something. The second characteristic is that you get a fixed-length output no matter what input is given. Finally, it should have few or no collisions. A collision is when two different inputs provide the same output.

Hash – cont.

- MD5
- SHA1
- SHA2
- SHA3

VERY Simple Illustration of Rainbow Tables

Password	MD5 Hash (in Hex)
aaaa	74b87337454200d4d33f80c4663dc5e5
aaab	4c189b020ceb022e0ecc42482802e2b8
aaac	3963a2ba65ac8eb1c6e2140460031925
aaa1	39dc4f1ee693e5adabddd872247e451f
aaa2	0ad346c93c16e85e2cb117ff1fcfada3
aaa4	ee93fca7c150d9c548aff721c87d0986

Password	MD5 Hash (in Hex)
aaaaa	594f803b380a41396ed63dca39503542
aaabb	120858a7016efcfab66967b834e9153c
aaacc	ee43671d755ac457cfe6e32d1894788e
aaa1a	5bbac29650eb36b4de16885c190a9fa3
aaa2a	597f0ce6d11567cc691b3f5df35594cb
aaa4a	4305dc076b3ba2bf8d55524cddf5a72d

Historical Steganography

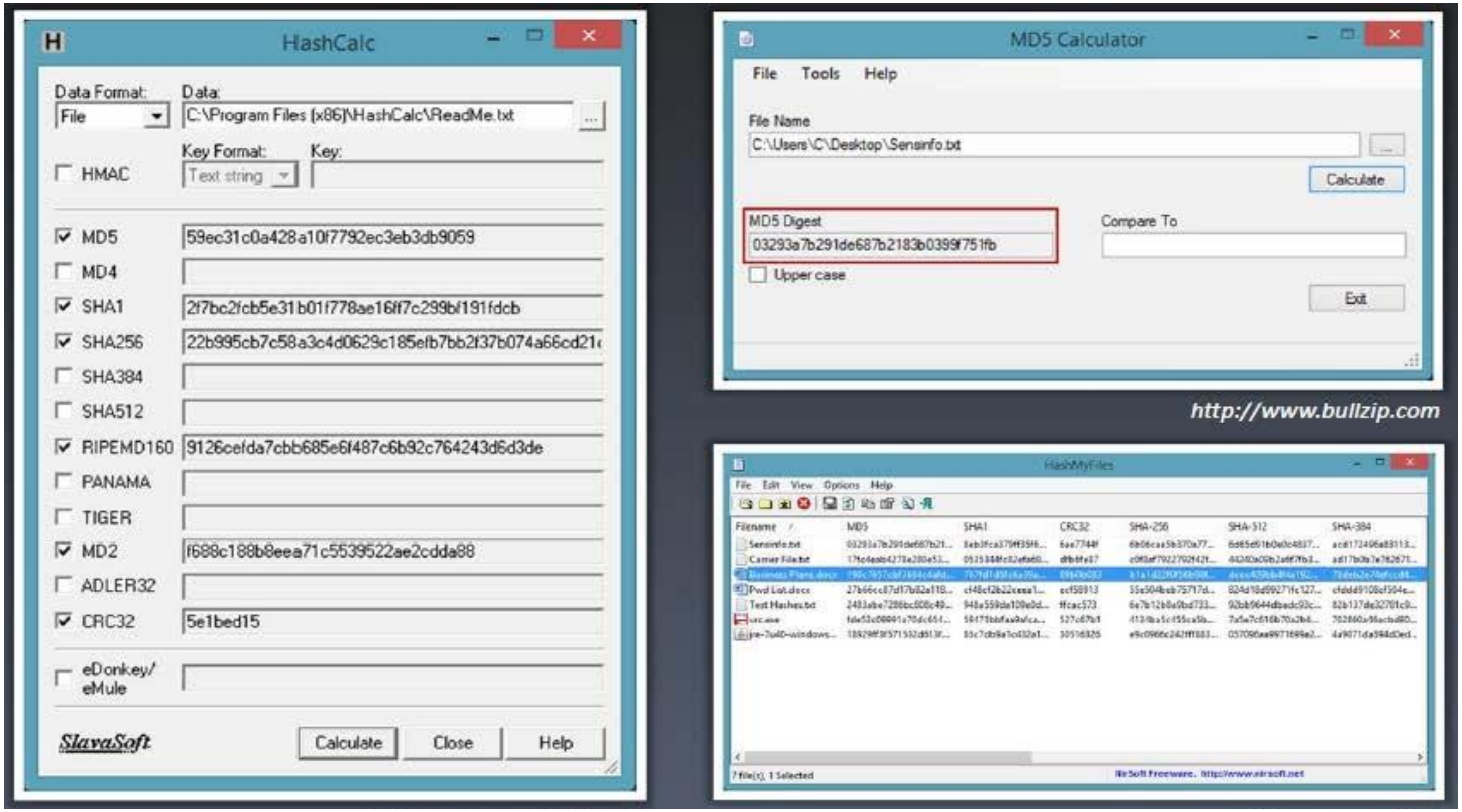
- The ancient Chinese wrapped notes in wax and swallowed them for transport.
- In ancient Greece a messenger’s head might be shaved, a message written on his head, then his hair was allowed to grow back.
- In 1518 Johannes Trithmeus wrote a book on cryptography and described a technique where a message was hidden by having each letter taken as a word from a specific column.

Ancient Greece-486BC

Historical Steganography - Continued

- During WW II the French Resistance sent messages written on the backs of couriers using invisible ink
- Microdots are images/undeveloped film the size of a typewriter period, embedded on an innocuous documents. These were said to be used by spy's during the Cold War.

MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles



Data Format: File

Data: C:\Program Files (x86)\HashCalc\ReadMe.txt

□ HMAC   Key Format: Text string   Key:

☑ MD5	59ec31c0a428a10f7792ec3eb3db9059
□ MD4	
☑ SHA1	2f7bc2fcb5e31b01f778ae16ff7c299bf191fdcb
☑ SHA256	22b995cb7c58a3c4d0629c185efb7bb2f37b074a66cd21
□ SHA384	
□ SHA512	
☑ RIPEMD160	9126cefda7cbb685e6f487c6b92c764243d6d3de
□ PANAMA	
□ TIGER	
☑ MD2	f688c188b8eea71c5539522ae2cdda88
□ ADLER32	
☑ CRC32	5e1bed15
□ eDonkey/ eMule	

File Name: C:\Users\C\Desktop\Sensinfo.txt

MD5 Digest: 03293a7b291de687b2183b0399f751fb

Compare To:

□ Upper case

http://www.bullzip.com

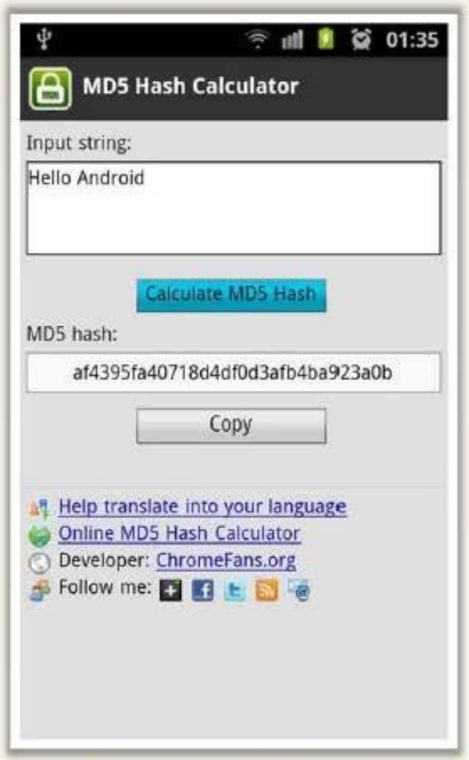
Filename	MD5	SHA1	CRC32	SHA-256	SHA-512	SHA-384
Sensinfo.txt	03293a7b291de687b21...	8eb3fca379ff35f6...	6ae7744f	6b06caa5b370a77...	6d65d91b0a0c4837...	acd172406a83113...
Career File.txt	17fc4eab4278a280e53...	0535344fc82efa60...	dfb8fe87	c0f0af7922792f42f...	44240a09b2a6f7b3...	ad17b0b7e762671...
Business Plans.docx	190c7657cbf7484cdafd...	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Pwd List.docx	27b66cc87d17b82a119...	cf48cf2b22ceea1...	ecf58913	55e504bcb75717d...	824d18d99271fc127...	cfddd9108cf504e...
Test Hashes.txt	2483abe7286bc808c49...	948a559da109e0d...	ffcac573	6e7b12b8a0bd733...	92bb9644dbadc93c...	82b137de32701c0...
src.exe	fde52c08991a70dc651...	58471bbfaa9afca...	527c67b1	413f8a5cf55ca5b...	7a5e7c616b70a2b6...	702860a96acbd80...
jre-7u40-windows...	18929ff3f571532d613f...	85c7db9a1c032a1...	30516325	e9c0966c242fff883...	057096aa99716 99e2...	4a9071da594d0ed...

7 file(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles

MD5 Hash Calculator



01:35

MD5 Hash Calculator

Input string:

Hello Android

Calculate MD5 Hash

MD5 hash:

af4395fa40718d4df0d3afb4ba923a0b

Copy

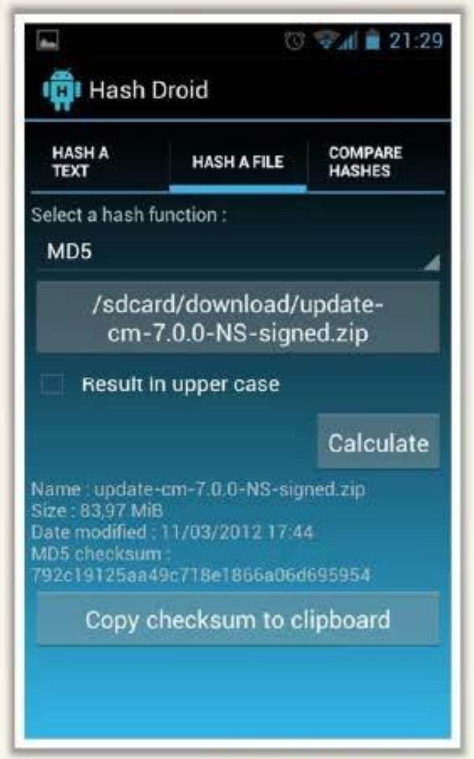
Help translate into your language

Online MD5 Hash Calculator

Developer: ChromeFans.org

Follow me:

Hash Droid



21:29

Hash Droid

HASH A TEXT | HASH A FILE | COMPARE HASHES

Select a hash function :

MD5

/sdcard/download/update-cm-7.0.0-NS-signed.zip

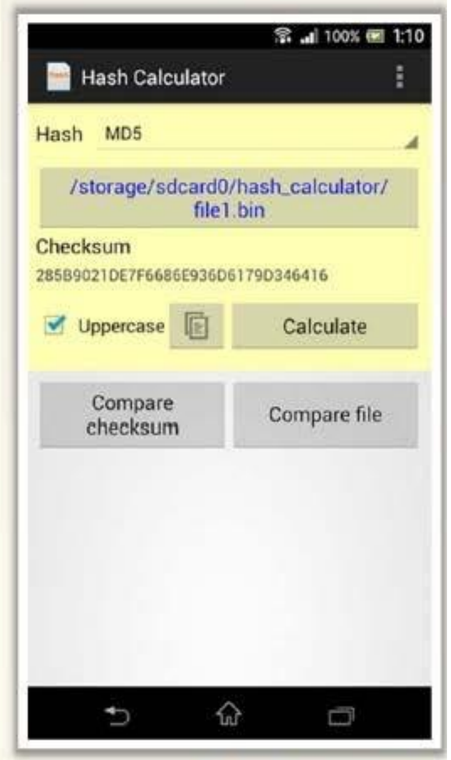
☐ Result in upper case

Calculate

```
Name : update-cm-7.0.0-NS-signed.zip
Size : 83,97 MiB
Date modified : 11/03/2012 17:44
MD5 checksum :
792c19125aa49c718e1866a06d695954
```

Copy checksum to clipboard

Hash Calculator



100% 1:10

Hash Calculator

Hash: MD5

/storage/sdcard0/hash_calculator/file1.bin

Checksum

285B9021DE7F6686E936D6179D346416

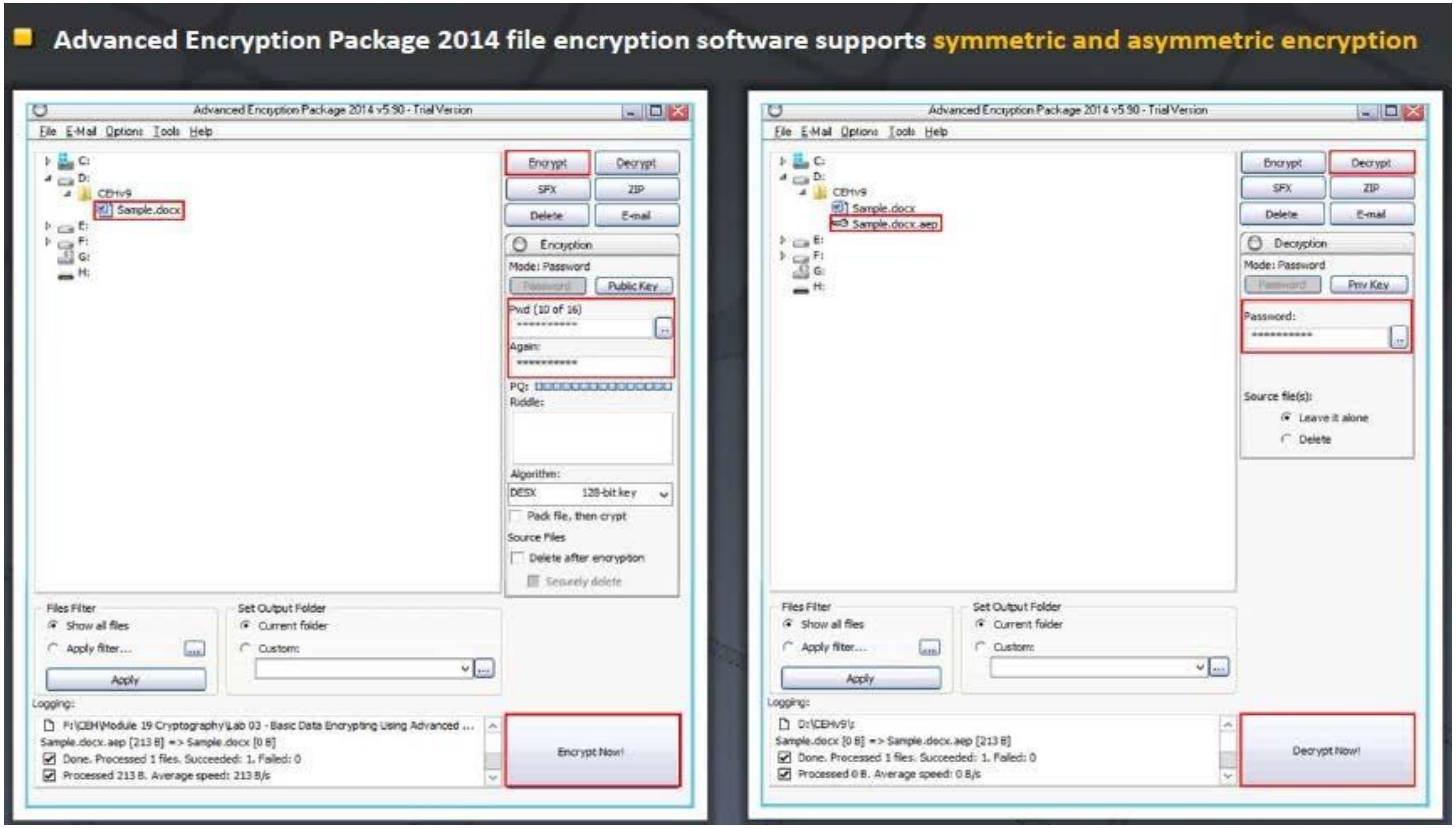
☑ Uppercase

Calculate

Compare checksum

Compare file

Cryptography Tool: Advanced Encryption Package 2014



- Advanced Encryption Package 2014 file encryption software supports **symmetric and asymmetric encryption**

Encryption

Mode: Password

Pwd (10 of 16): ***********

Again: ***********

PQ:

Riddle:

Algorithm: DESX 128-bit key

□ Pack file, then crypt

Source Files

□ Delete after encryption

□ Securely delete

Files Filter: ● Show all files ○ Apply filter...

Set Output Folder: ● Current folder ○ Custom:

Logging:

```
F:\CEH\Module 19 Cryptography\Lab 03 - Basic Data Encrypting Using Advanced ...
Sample.docx.aep [213 B] => Sample.docx [0 B]
☑ Done. Processed 1 files. Succeeded: 1. Failed: 0
☑ Processed 213 B. Average speed: 213 B/s
```

Decryption

Mode: Password

Password: ***********

Source file(s): ● Leave it alone ○ Delete

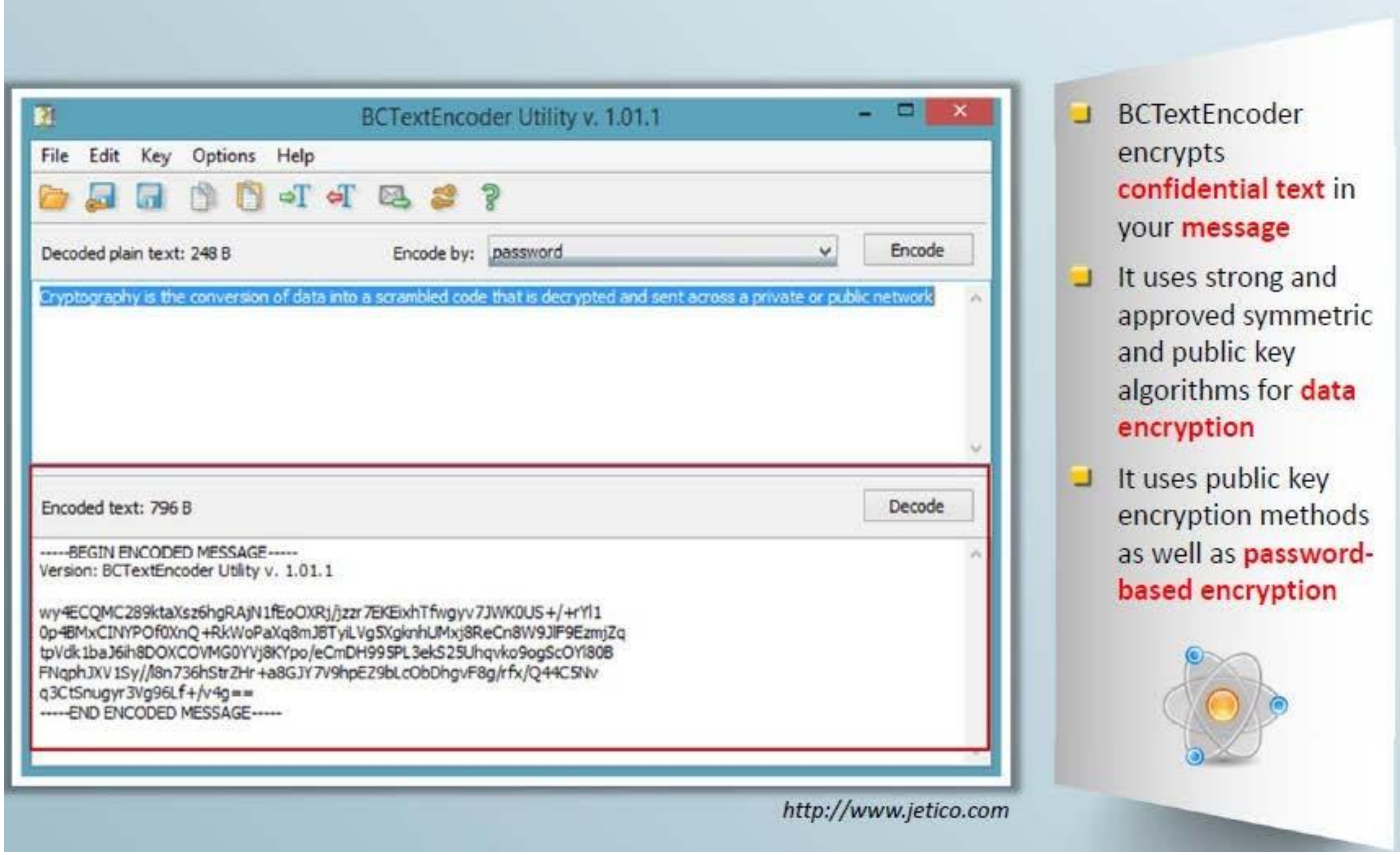
Files Filter: ● Show all files ○ Apply filter...

Set Output Folder: ● Current folder ○ Custom:

Logging:

```
D:\CEHv9\:
Sample.docx [0 B] => Sample.docx.aep [213 B]
☑ Done. Processed 1 files. Succeeded: 1. Failed: 0
☑ Processed 0 B. Average speed: 0 B/s
```

Cryptography Tool: BCTextEncoder



Decoded plain text: 248 B

Encode by: password

Cryptography is the conversion of data into a scrambled code that is decrypted and sent across a private or public network

Encoded text: 796 B

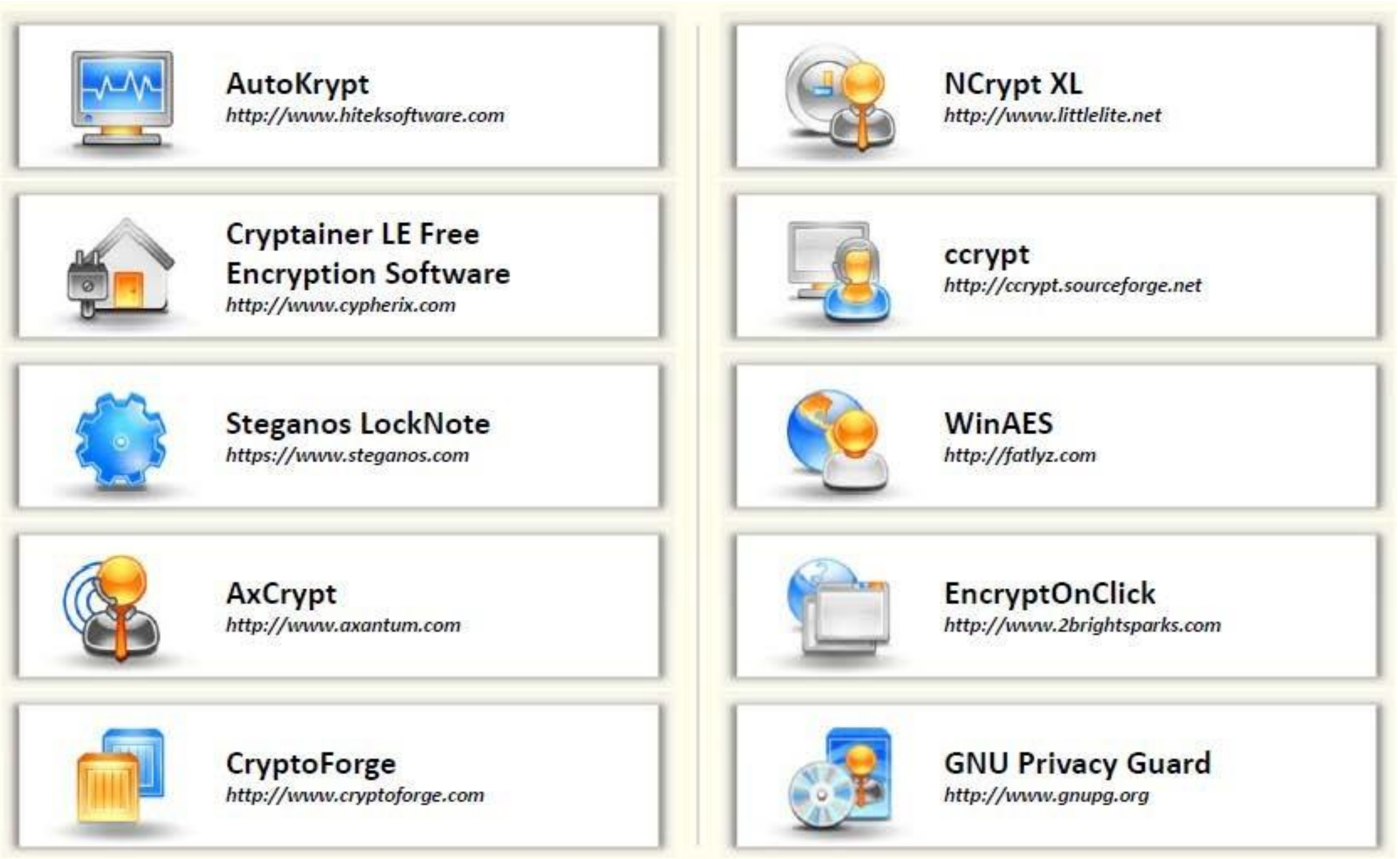
```
-----BEGIN ENCODED MESSAGE-----
Version: BCTextEncoder Utility v. 1.01.1

wy4ECQMC289ktaXsz6hgRAjN1fEoOXRj/jzzr7EKEixhTfwgyv7JWK0US+/+rYl1
0p4BMxCINYPOf0XnQ+RkWoPaXq8mJBTyiLVg5XgknhUMxj8ReCn8W9JlF9EzmjZq
tpVdk1baJ6ih8DOXCOVMG0YVj8KYpo/eCmDH995PL3ekS25Uhqvko9ogScOYl80B
FNqphJXV1Sy//l8n736hStrZHr+a8GJY7V9hpEZ9bLcObDhgvF8g/rfx/Q44C5Nv
q3CtSnugyr3Vg96Lf+/v4g==
-----END ENCODED MESSAGE-----
```

http://www.jetico.com

- BCTextEncoder encrypts **confidential text** in your **message**
- It uses strong and approved symmetric and public key algorithms for **data encryption**
- It uses public key encryption methods as well as **password-based encryption**

Cryptography Tools



AutoKrypt
http://www.hiteksoftware.com

Cryptainer LE Free Encryption Software
http://www.cypherix.com

Steganos LockNote
https://www.steganos.com

AxCrypt
http://www.axantum.com

CryptoForge
http://www.cryptoforge.com

NCrypt XL
http://www.littlelite.net

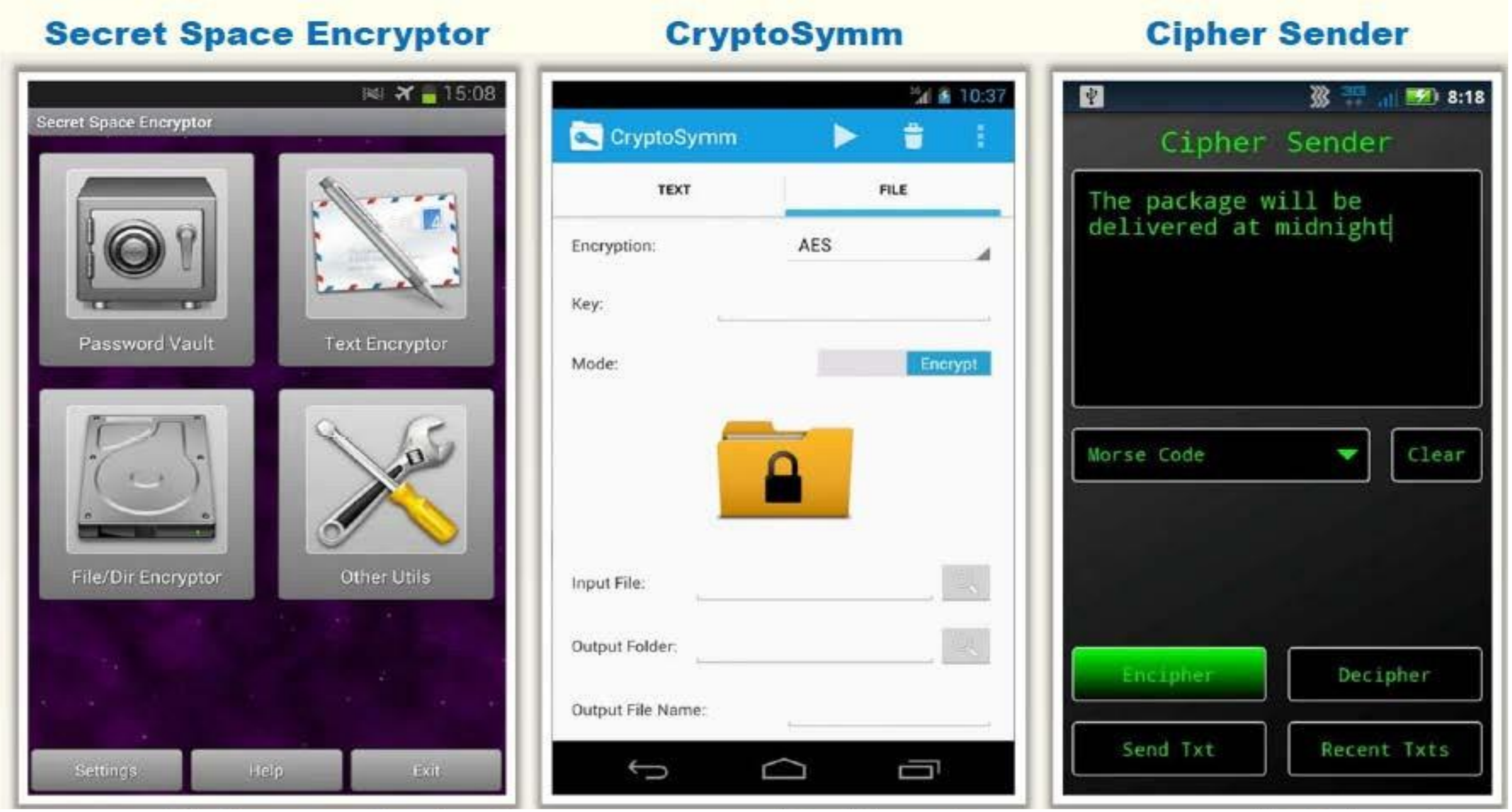
ccrypt
http://ccrypt.sourceforge.net

WinAES
http://fatlyz.com

EncryptOnClick
http://www.2brightsparks.com

GNU Privacy Guard
http://www.gnupg.org

Cryptography Tools for Mobile: Secret Space Encryptor, CryptoSymm and Cipher Sender



Secret Space Encryptor

CryptoSymm

Cipher Sender

Encryption: AES

Mode: Encrypt

The package will be delivered at midnight

Morse Code

Summary

- Encryption is a basic element of security.
- Encrypting data when transmitting is an integral part of any security plan.