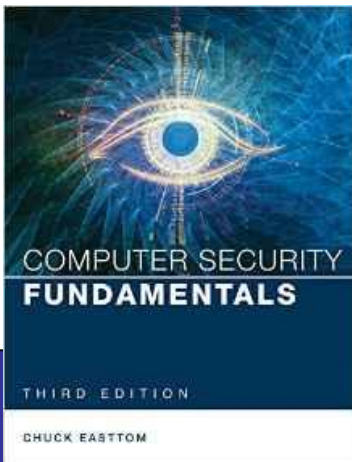


Computer Security Fundamentals

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.

Ancient Greece-486BC



■ 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

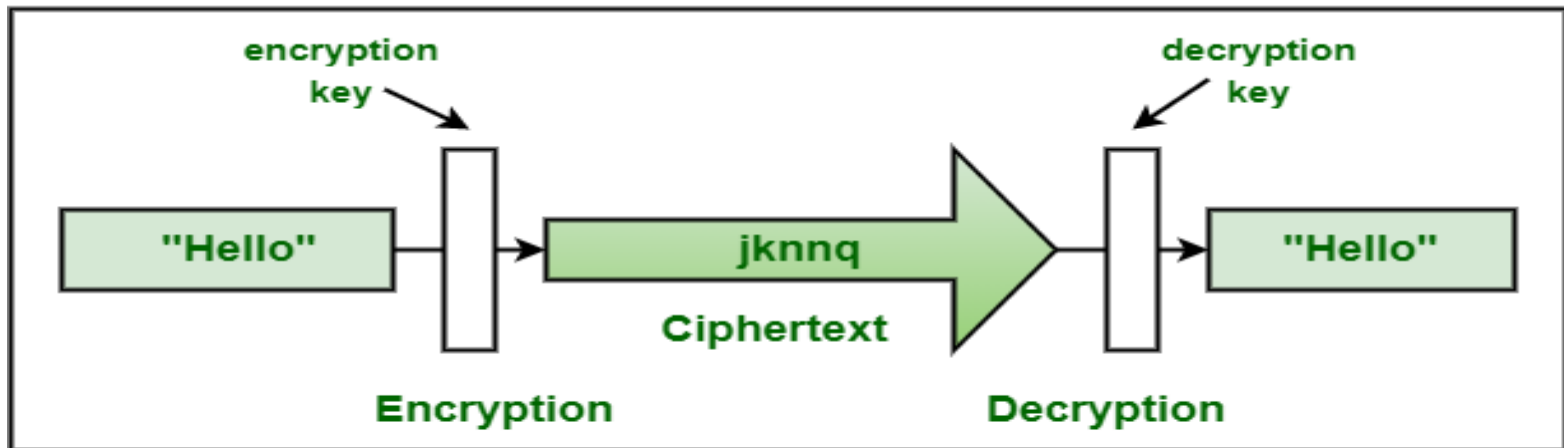


04

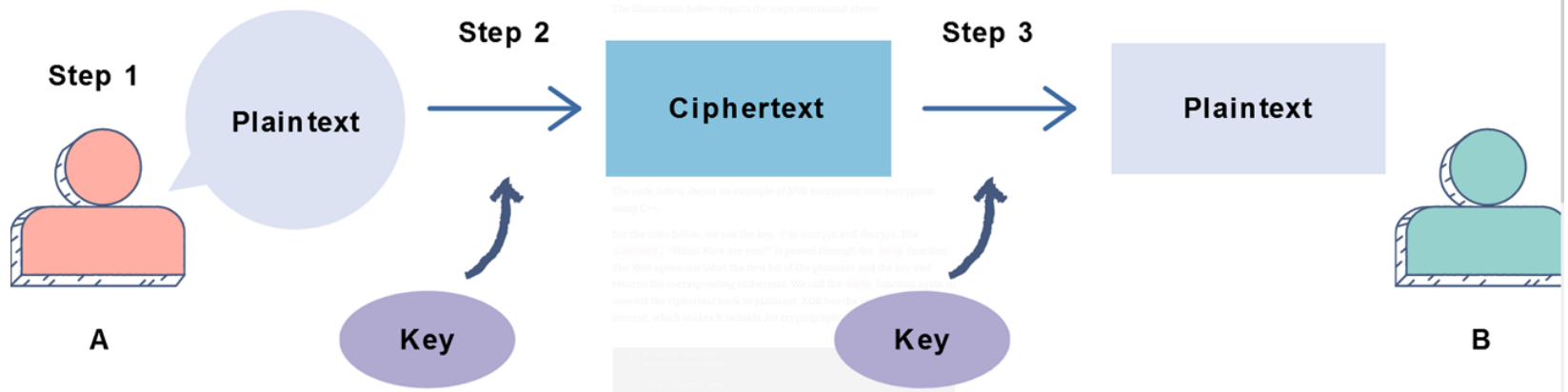




Encryption



Cryptography



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

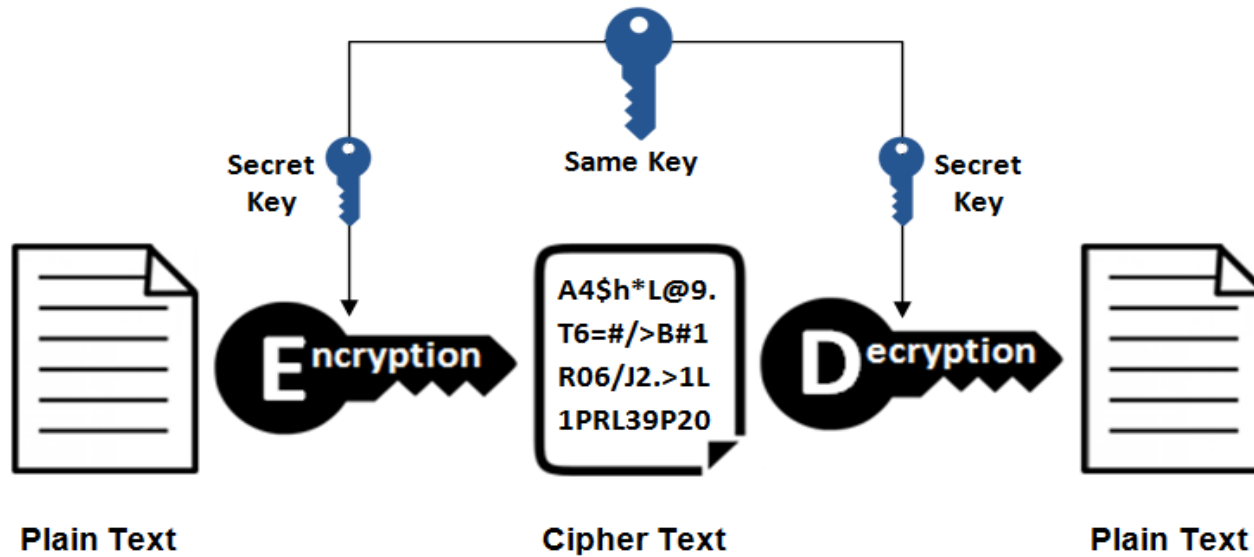


Asymmetric Encryption

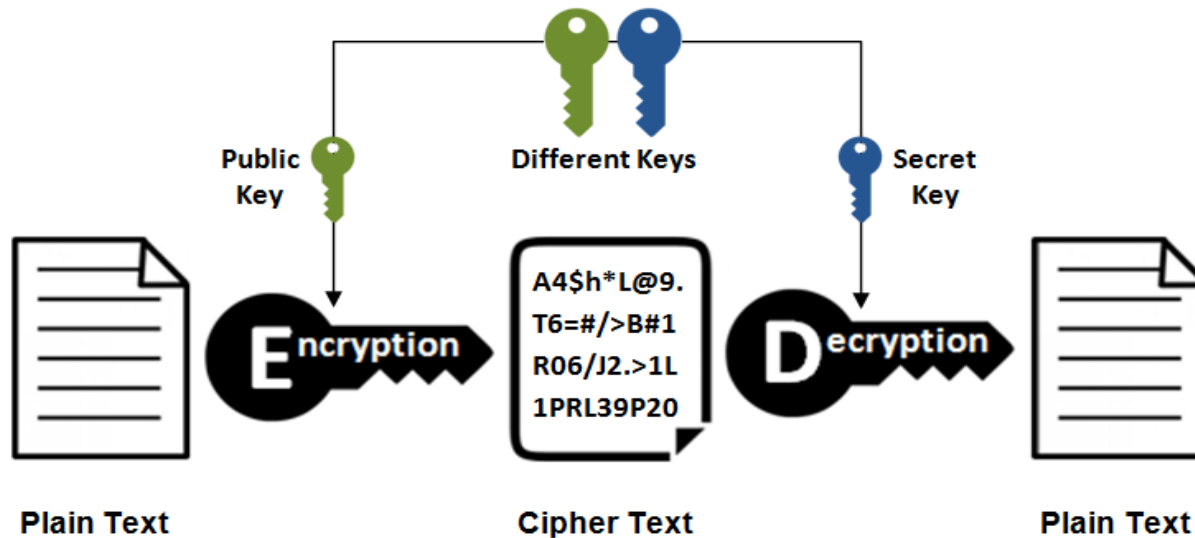
Asymmetric encryption (public-key) **uses different encryption keys** for encryption and decryption. These keys are known as public and private keys

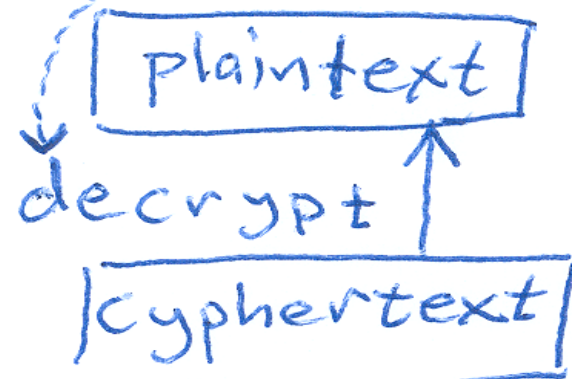
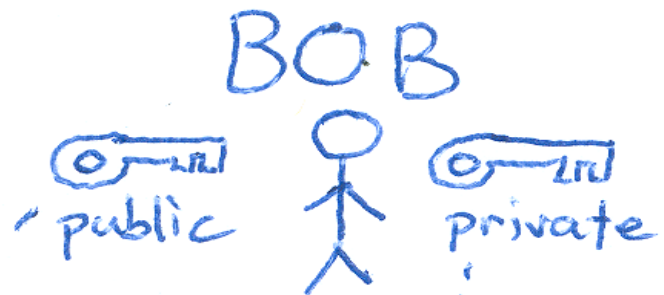
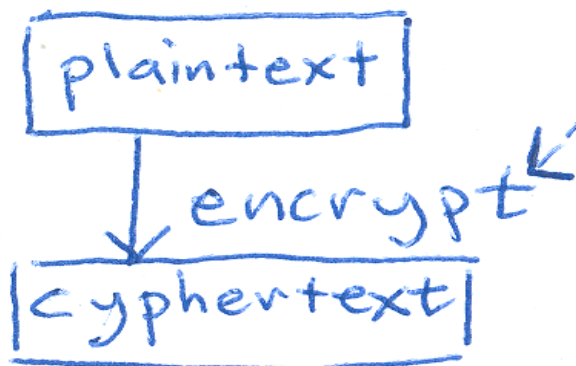


Symmetric Encryption



Asymmetric Encryption





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

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

Binary Operations

- Example of OR operation

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

Binary Operations

- Example of XOR operation

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

Binary Operations

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

A DOG = 065 032 068 079 071

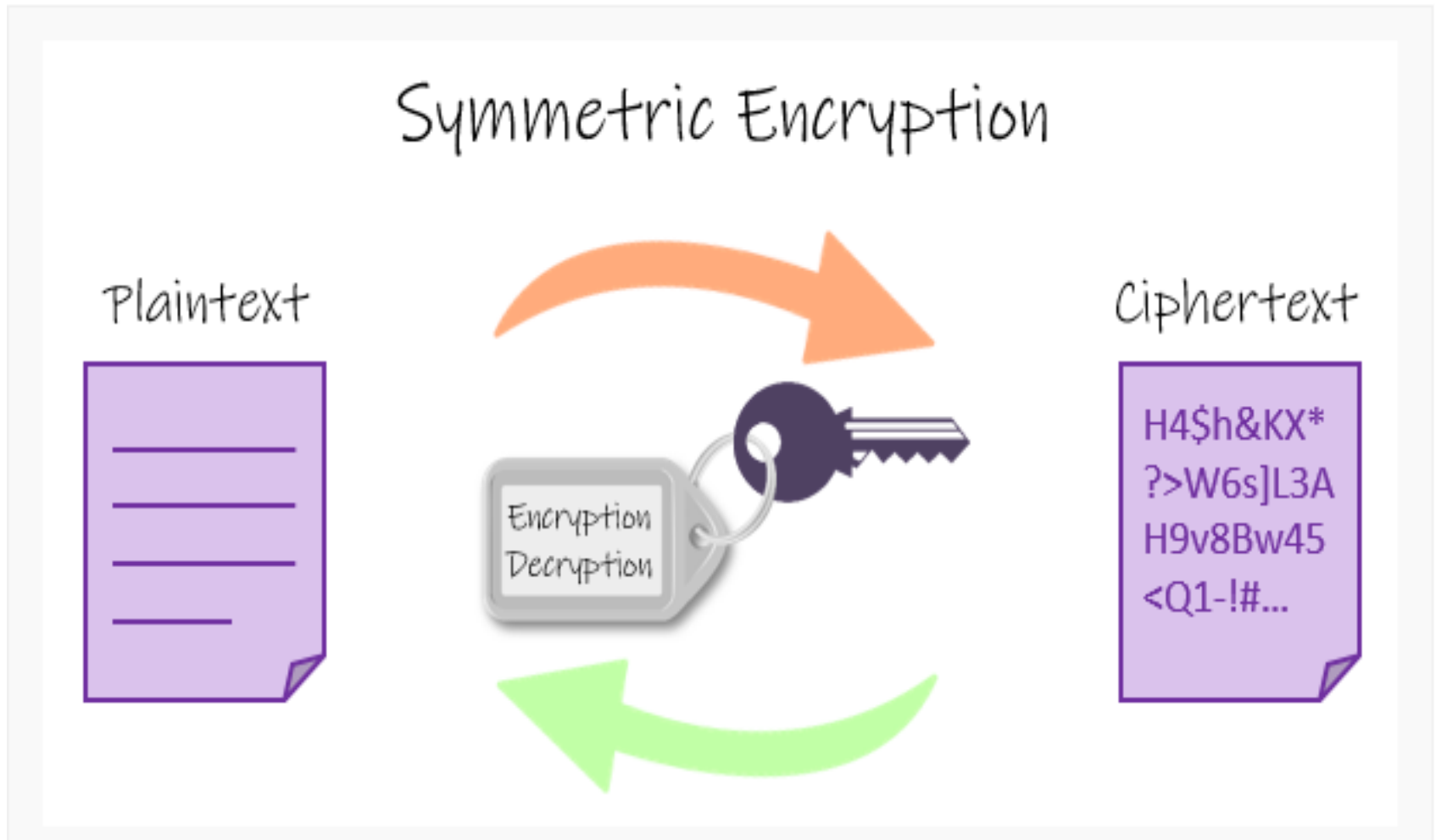
- Then, convert ASCII to binary

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



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.)

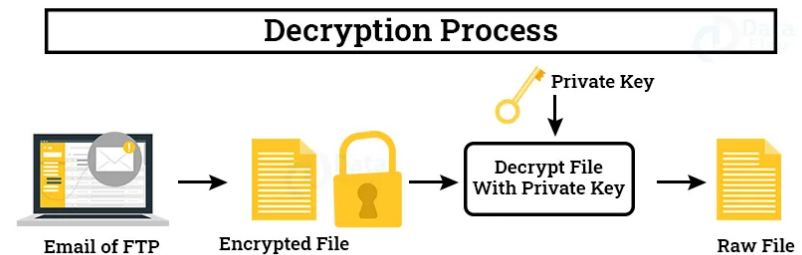
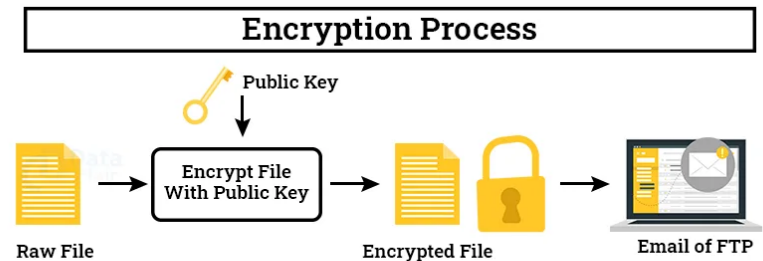
- Public key (asymmetric) encryption
 - Opposite of single key encryption.
 - One key (public key) used to encrypt .
 - One key (private key) used to decrypt.
 - Only holder of a private key can decrypt messages.

Modern Methods (cont.)

- Public key (asymmetric) encryption
 - Public key encryption is most widely used.

Modern Methods (cont.)

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



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 .
- You are 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.)



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

Modern Methods (cont.)

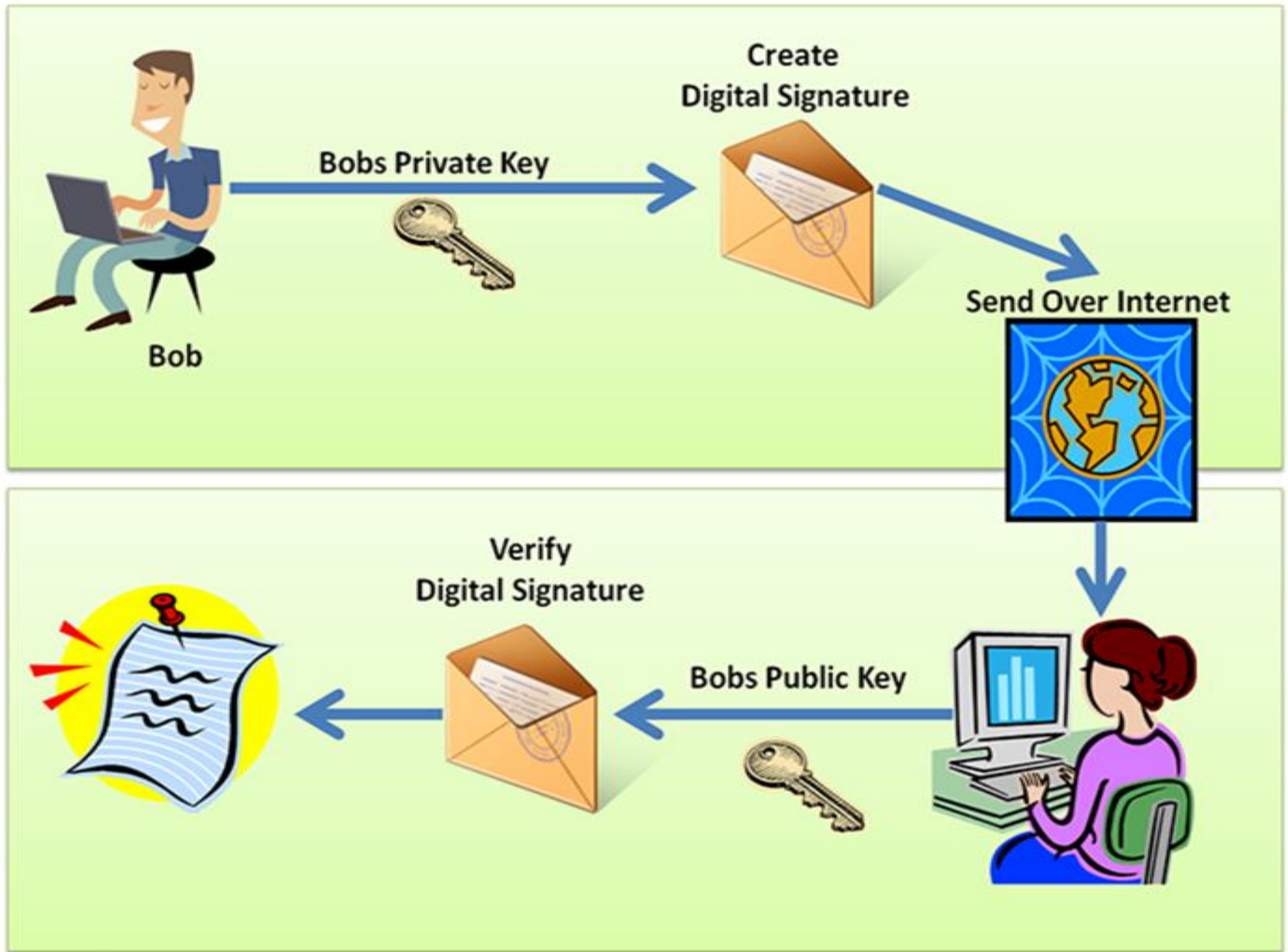
- Legitimate versus fraudulent encryption
 - Warning signs of frauds
 - Unbreakable
 - Certified
 - Inexperienced people

Avoid 'bad' crypto

- Unbreakable
- Unhackable
- Secret algorithm
- Kerhoff's principle

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.

Hash – cont.

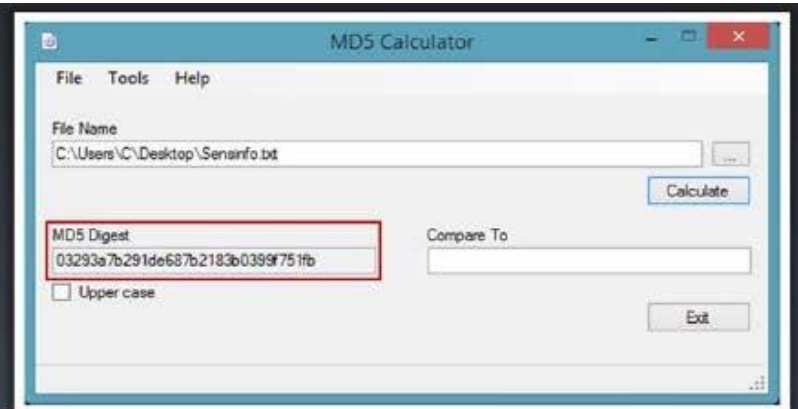
- MD5
- SHA1
- SHA2
- SHA3

VERY Simple Illustration of Rainbow Tables

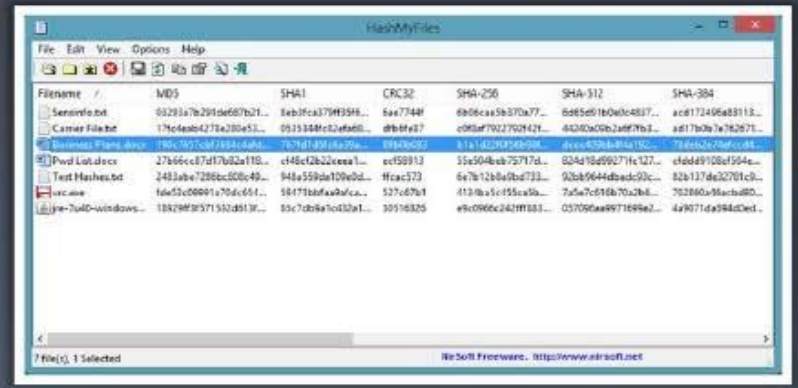
Password	MD5 Hash (in Hex)
aaaa	74b87337454200d4d33f80c4663dc5e5
aaab	4c189b020ceb022e0ec c42482802e2b8
aaac	3963a2ba65ac8eb1c6e 2140460031925
aaa1	39dc4f1ee693e5adabd dd872247e451f
aaa2	0ad346c93c16e85e2cb 117ff1fcfada3
aaa4	ee93fca7c150d9c548af f721c87d0986

Password	MD5 Hash (in Hex)
aaaaa	594f803b380a41396ed 63dca39503542
aaabb	120858a7016efcfab669 67b834e9153c
aaacc	ee43671d755ac457cfe 6e32d1894788e
aaa1a	5bbac29650eb36b4de1 6885c190a9fa3
aaa2a	597f0ce6d11567cc691b 3f5df35594cb
aaa4a	4305dc076b3ba2bf8d5 5524cddf5a72d

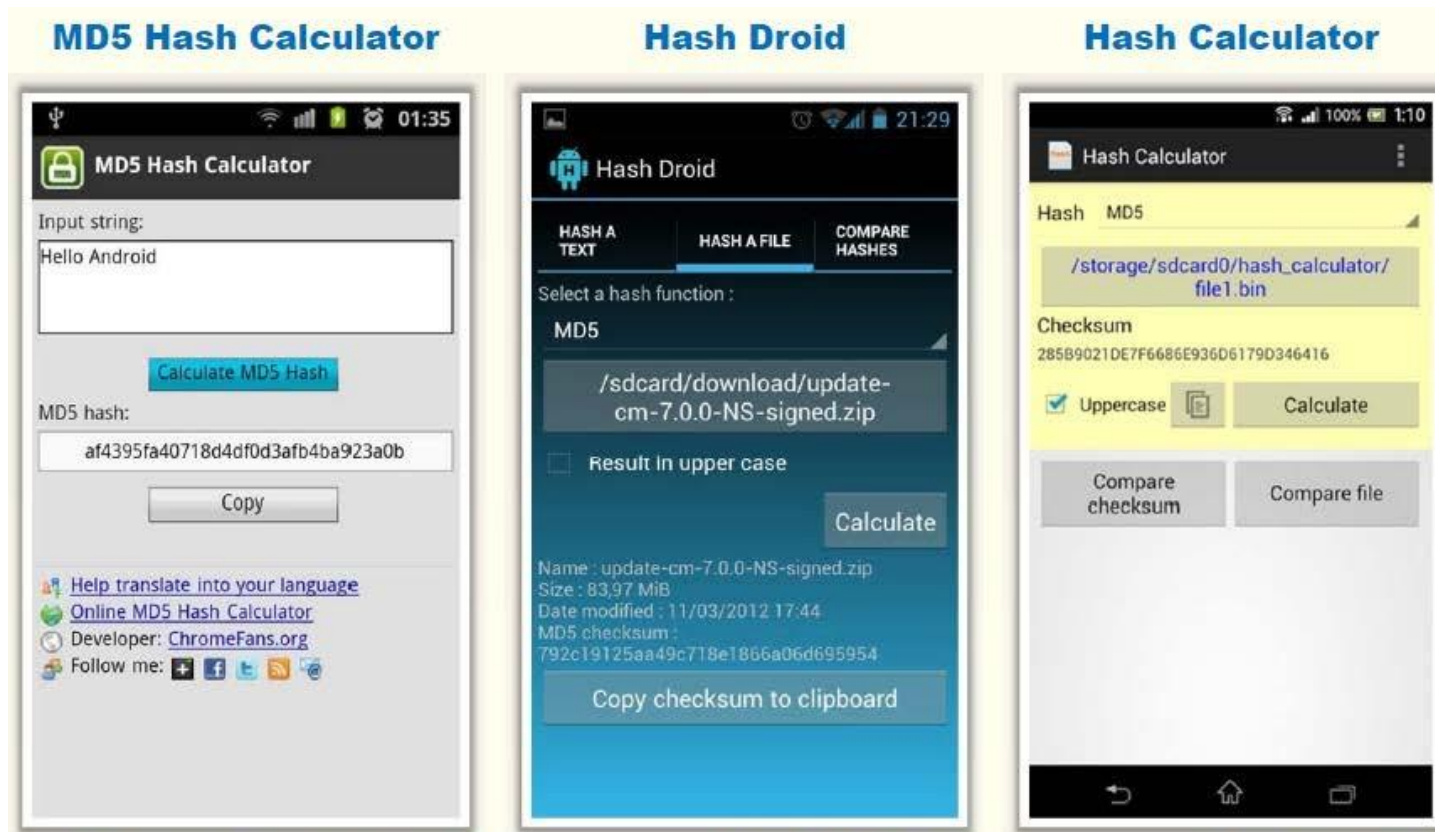
MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles



<http://www.bullzip.com>

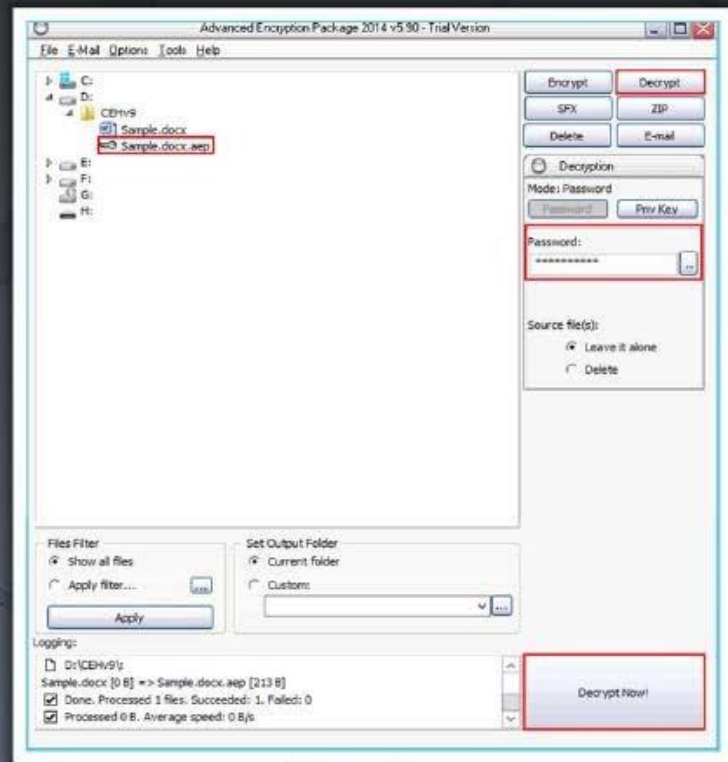
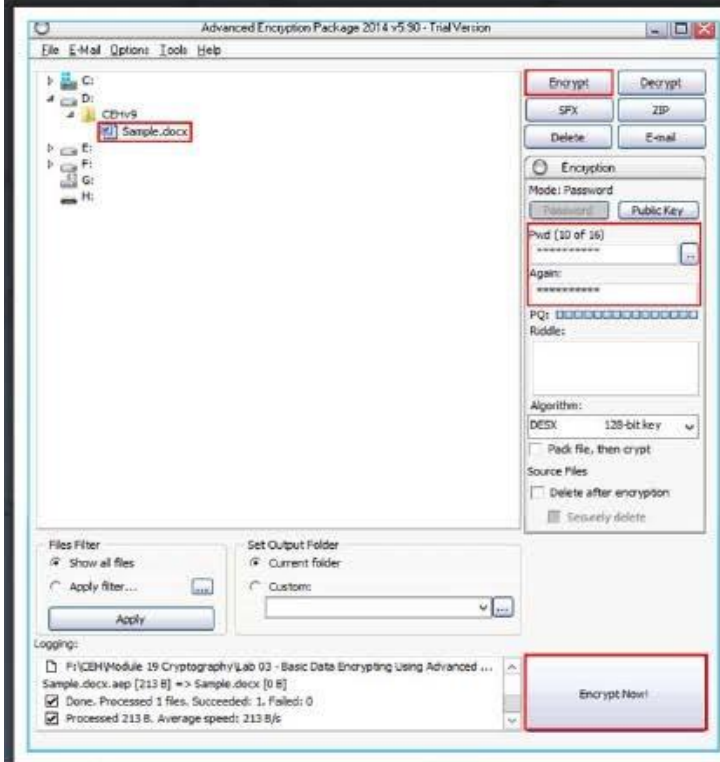


MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles

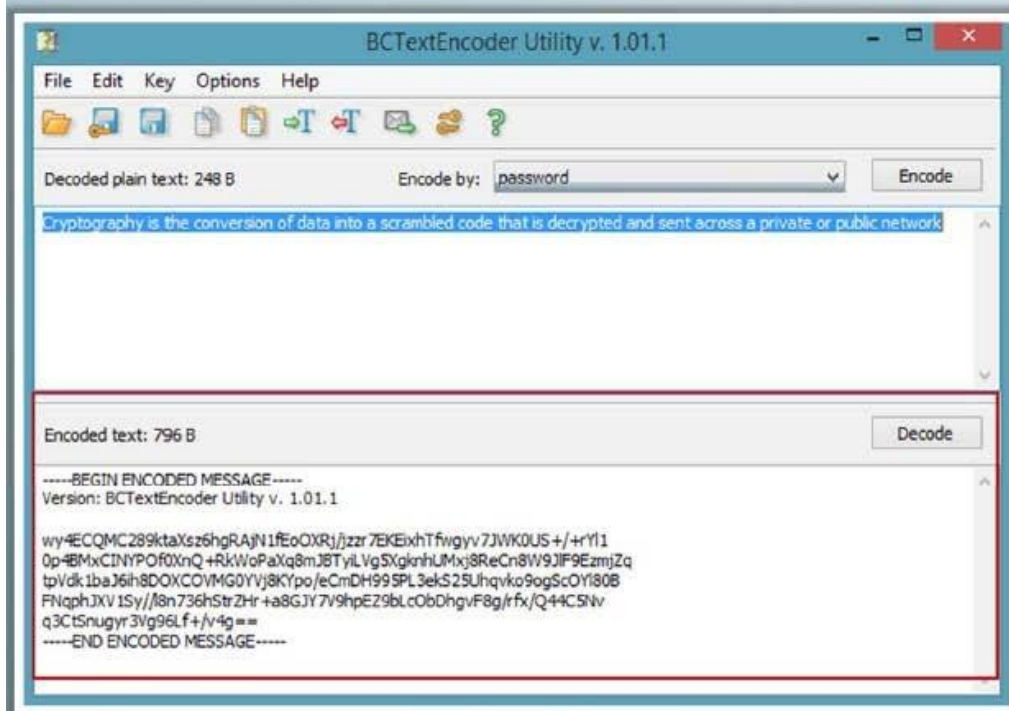


Cryptography Tool: Advanced Encryption Package 2014

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



Cryptography Tool: BCTextEncoder



<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>



NCrypt XL

<http://www.littlelite.net>



**Cryptainer LE Free
Encryption Software**

<http://www.cypherix.com>



ccrypt

<http://ccrypt.sourceforge.net>



Steganos LockNote

<https://www.steganos.com>



WinAES

<http://fatlyz.com>



AxCrypt

<http://www.axantum.com>



EncryptOnClick

<http://www.2brightsparks.com>



CryptoForge

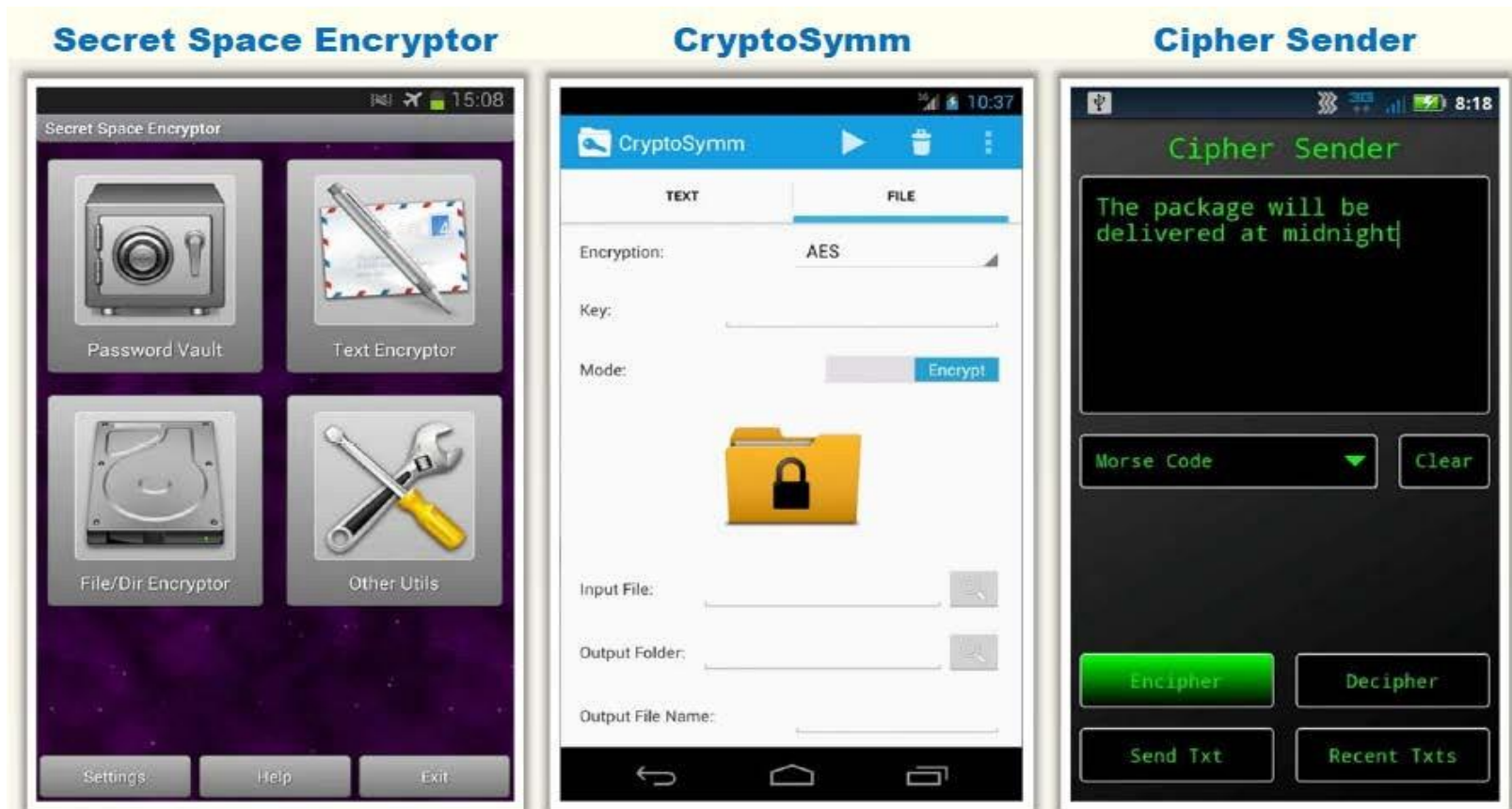
<http://www.cryptoforge.com>



GNU Privacy Guard

<http://www.gnupg.org>

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



Summary

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