



Cryptography

Module 18

Unmask the Invisible Hacker.



Market Survey 2014: The Year of Encryption



60% of those surveyed said that Edward Snowden revelations have made them more aware of data security



Among the 60%, approximately **70%** have been directly influenced to look at new data security systems



94% of people looking to invest in new systems are specifically examining secure (encryption) electronic data security systems



Only **17%** of those surveyed said their existing secure information sharing system was easy to use



100% of those not interested in security systems admitted to regularly sharing sensitive/ confidential data with external third parties



Over **2/3** of people felt that government certification combined with ease of use would be deciding factors when selecting a data security solution



One in two people now perceive the Cloud to be less secure as result of Snowden



One third of those surveyed were not that upcoming EU DPA reforms would impact the way they or their organization handles and protects data

<http://www.egress.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study: Heartbleed



Heartbleed is a security flaw in the **OpenSSL** cryptographic software library, which allows data traversal over **SSL/TLS in plain-text**

Heartbleed exploits a built-in feature of OpenSSL called **heartbeat**

Attackers exploit this vulnerability to get information such as OpenSSL **private keys**, OpenSSL **secondary keys**, up to **64kb of memory** from the affected server, **usernames** and **passwords**, etc.

Versions of OpenSSL affected by Heartbleed include **1.0.1** to **1.0.1f**

Updating OpenSSL to version **1.0.1g** or **higher** resolves the vulnerability

```
root@root:~#
File Edit View Search Terminal Help
msf auxiliary(openssl_heartbleed) > [exploit]
[*] 10.0.0.3:443 - Sending Client Hello...
[*] 10.0.0.3:443 - Sending Heartbeat...
[*] 10.0.0.3:443 - Heartbeat response, 65551 bytes
[+] 10.0.0.3:443 - Heartbeat response with leak
[*] 10.0.0.3:443 - Printable info leaked: S@eLxx0af"!98532ED/Atml+xml,application/xm
l;q=0.9,image/webp,*/*;q=0.8User-Agent: Mozilla/5.0 (Windows NT 6.0; W0W64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36Referer: https://localhost/owncloud/Accept-Encoding: gzip,deflate,sdchAccept-Language: en-US,en;q=0.8Cookie: oodhq3yekxnw=6c9e01ba193j14bh366179b0k4use#share=florida%401235timezone-offset=-7(NJ,"B4U#Wb[Yk")T13Pxyh3n",94r-6186#Y+00G0'!mTy>4[cest/J#01g=c74+)AC$#Wt@#yD@PIA]KyX
<sd+.-B*:\'C<GqKbnD^4!k,>ZfmEZU=>KK<m.xxCHuK*zsipu)y)i?E_>r7zVMb+6WMDRj7b|g+HIA*
08c)+bm-YFc,*V5L=i?7HM0r79%Wjzv'9NL'i</-6;0=q=G>|V:142s64v)VyHMs#337E
UNC.8X(X'8ug0g*)djWU[;31k&."h@+i.B+>ZMh%gg<:ChE<0\BrJu0#kqqKcsPt&fZ @vW@C0YLH 5
NB* Y=30BkxkqEwhyp28u?il&,Y;#zn l"yLvx3-LHiw0Dlzf;Mk{826}<|g@aQJ02h]>C|E{sg(j;)zq
B9|[1]FeMrj%;."rt<el*rk)-33h(*1e0).DSmXv@8*+62Sg%Zj8<0:$00F,-0@*H@10UUS1@UFlorida
100UMiam110UABC10UDEF1@localhost:10087#H)riniamatthews@gmail.com01468201244472150820124
4472810UUS1@UFlorida1@UMiami110UABC10UDEF1@localhost:10087#Hriniamatthews@gmail.com00*
H0(> %>ue4>#oxe@l!v4/:?Se<cmFgu102ij0@2]rZMz4)@1w0#He5B0#K5q!rg 8SAX3v4' (X:>2<AdUwg
gK $7)KV7 <{s}vAHZMEI28aL399yE4>,0-bv>526 UR'u"sa4"hLW gn@<#04WJF|%(<#0>+16r)w15
"6..vCK74r,/'``B.033=AzvIr6:'F;78%6 ! MPR7x'e?@%kgw*d[p' cDg/XsrvGlivg9i?rxK@8d4j;y
wGaW()mTy077:;! "gvr1508201244720180UUS1@UFlorida1@UMiami110UABC10UDEF1@localhost:10087#H)riniamatthews@gmail.com00*H0(> %>ue4>#oxe@l!v4/:?Se<cmFgu102ij0@2]rZMz4)@1w0#He
5B0#K5q!rg 8SAX3v4' (X:>2<AdUwgK $7)KV7 <{s}vAc*>#M0Bnh+;Ue$60*,%Lm&p04x7fb..110
"97:#NFID1@#T?u;C5..NAn?/Oyno&g*W95;aKmrR:U0D /qzf(3pwn,X->8ad1{jLN0%YCA}D6<ow(F>
q abW5f#LIDL285frf@1a|r=<zqIky49uJTF[l@gu'CI/XC/@g2]C]A/rugXwmv*EW0#A2-\$0R[P0 44
4a4562987854f219a124f826a750c,Sop\33uq6ul0! I 444a4562987854f219a124f826a750c,SuqDu
qZuqpE/''3uquququq@uquququq
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Case Study: Poodlebleed



- Poodlebleed (**Padding Oracle On Downgraded Legacy Encryption**) is a security vulnerability in the design of SSL 3.0
- Attacker exploits this vulnerability to **decrypt ciphertext in transit** between a server and a browser, by means of padding oracle side-channel attack
- **Countermeasures:**
 - Completely **disable SSL 3.0** on the client side and the server side
 - Implement **anti-POODLE record splitting**



<https://poodlebleed.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives



- Understanding Cryptography Concepts
- Overview of Encryption Algorithms
- Cryptography Tools
- Understanding Public Key Infrastructure (PKI)



- Understanding Email Encryption
- Understanding Disk Encryption
- Understanding Cryptography Attacks
- Cryptanalysis Tools



Module Flow



1

Cryptography Concepts

2

Encryption Algorithms

3

Cryptography Tools

4

Public Key Infrastructure (PKI)

5

Email Encryption

6

Disk Encryption

7

Cryptography Attacks

8

Cryptanalysis Tools

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.



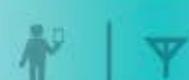
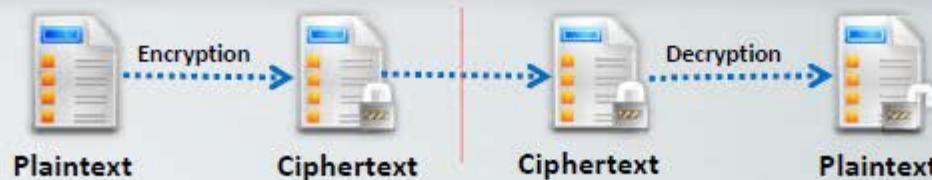
03

Objectives

- Confidentiality
- Integrity
- Authentication
- Non-repudiation



04

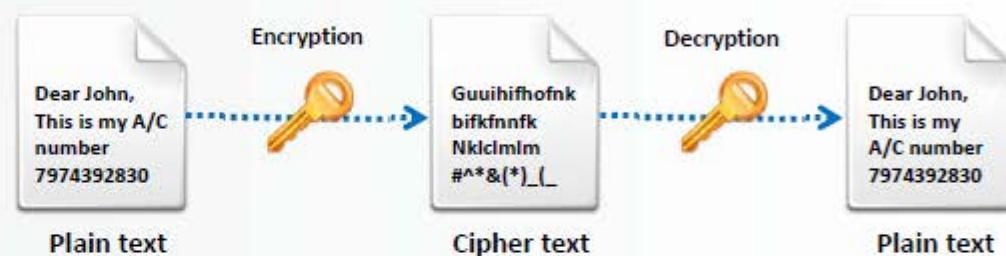


Types of Cryptography



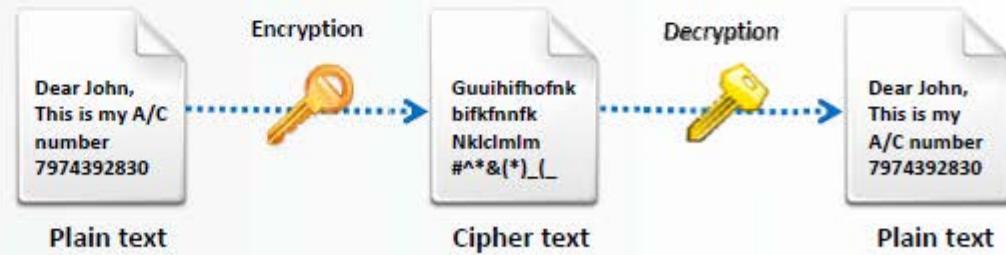
Symmetric Encryption

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



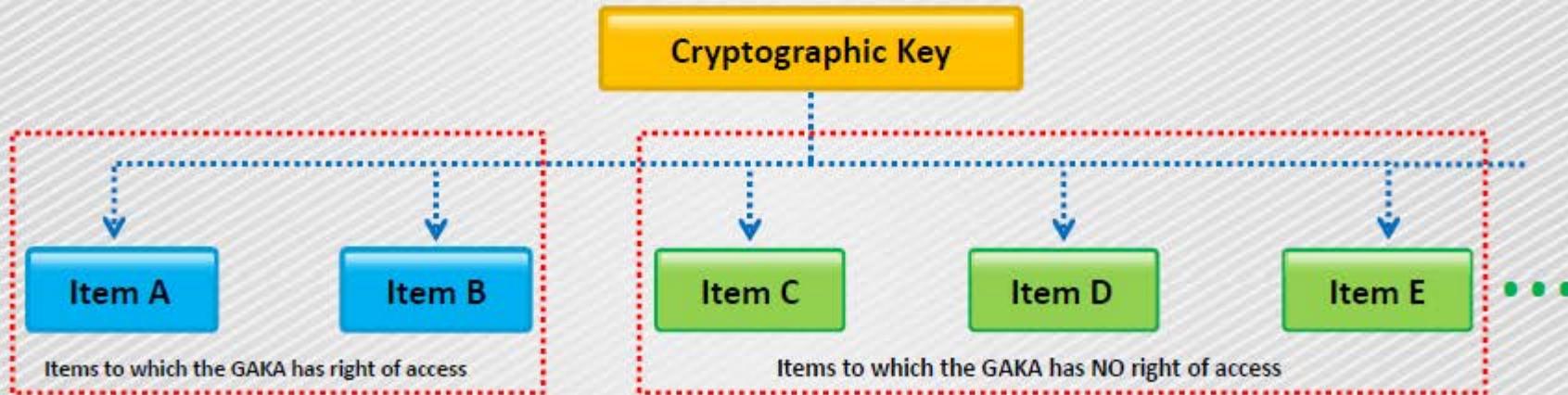
Government Access to Keys (GAK)



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**



Module Flow



1

Cryptography Concepts

2

Encryption Algorithms

3

Cryptography Tools

4

Public Key Infrastructure (PKI)

5

Email Encryption

6

Disk Encryption

7

Cryptography Attacks

8

Cryptanalysis Tools

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

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
```

RC4, RC5, RC6 Algorithms



RC4

A variable **key size stream cipher** with byte-oriented operations, and is based on the use of a random permutation



RC5

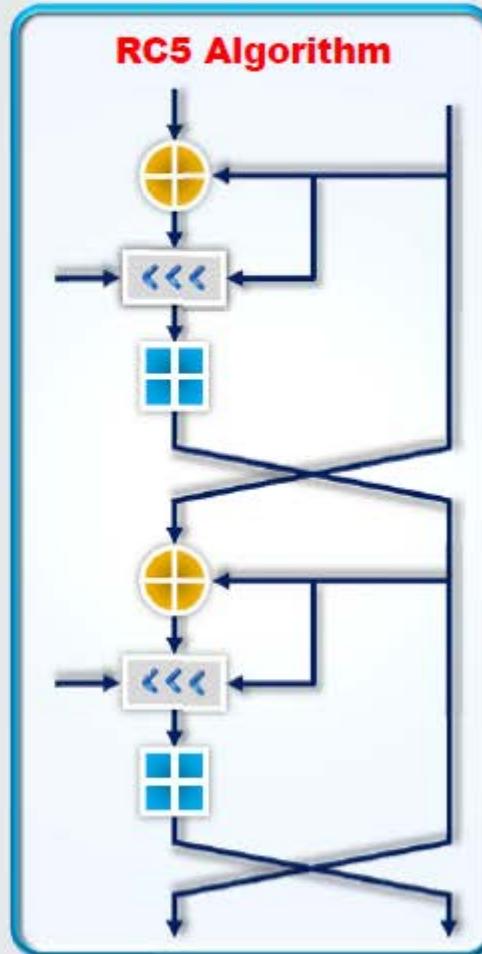
It is a **parameterized algorithm** with a variable block size, a variable key size, and a variable number of rounds. The key size is **128-bits**



RC6

RC6 is a **symmetric key block cipher** derived from RC5 with two additional features:

- Uses **Integer multiplication**
- Uses **four 4-bit working registers** (RC5 uses two 2-bit registers)



The DSA and Related Signature Schemes



Digital Signature Algorithm

FIPS 186-2 specifies the Digital Signature Algorithm (DSA) that may be used in the **generation and verification of digital signatures** for sensitive, unclassified applications

Digital Signature

The digital signature is **computed using a set of rules** (i.e., the DSA) **and a set of parameters** such that the identity of the signatory and integrity of the data can be verified

Each entity creates a public key and corresponding private key

1. Select a prime number q such that $2^{159} < q < 2^{160}$
2. Choose t so that $0 \leq t \leq 8$
3. Select a prime number p such that $2^{511+64t} < p < 2^{512+64t}$ with the additional property that q divides $(p-1)$
4. Select a generator α of the unique cyclic group of order q in Z_p^*
5. To compute α , select an element g in Z_p^* and compute $g^{(p-1)/q} \bmod p$
6. If $\alpha = 1$, perform step five again with a different g
7. Select a random a such that $1 \leq a \leq q-1$
8. Compute $y = \alpha^a \bmod p$



The public key is (p, q, α, y) . The private key is a .

RSA (Rivest Shamir Adleman)



RSA is an **Internet encryption and authentication system** that uses an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman

01



RSA encryption is widely used and is one of the **de-facto encryption standard**

02



It uses **modular arithmetic** and **elementary number theories** to perform computations using two large prime numbers

03



The RSA Signature Scheme



Algorithm Key generation for the RSA signature scheme

SUMMARY: each entity creates an RSA public key and a corresponding private key.
Each entity A should do the following:

1. Generate two large distinct random primes p and q , each roughly the same size.
2. Compute $n = pq$ and $\phi = (p - 1)(q - 1)$.
3. Select a random integer e , $1 < e < \phi$, such that $\gcd(e, \phi) = 1$.
4. Use the extended Euclidean algorithm (Algorithm 2.107) to compute the unique integer d , $1 < d < \phi$, such that $ed \equiv 1 \pmod{\phi}$.
5. A's public key is (n, e) ; A's private key is d .



Algorithm RSA signature generation and verification

SUMMARY: entity A signs a message $m \in \mathcal{M}$. Any entity B can verify A's signature and recover the message m from the signature.

1. *Signature generation.* Entity A should do the following:
 - (a) Compute $\tilde{m} = R(m)$, an integer in the range $[0, n - 1]$.
 - (b) Compute $s = \tilde{m}^d \pmod{n}$.
 - (c) A's signature for m is s .
2. *Verification.* To verify A's signature s and recover the message m , B should:
 - (a) Obtain A's authentic public key (n, e) .
 - (b) Compute $\tilde{m} = s^e \pmod{n}$.
 - (c) Verify that $\tilde{m} \in \mathcal{M}_R$; if not, reject the signature.
 - (d) Recover $m = R^{-1}(\tilde{m})$.

Example of RSA Algorithm



```
P = 61    <= first prime number (destroy this after computing E and D)
Q = 53    <= second prime number (destroy this after computing E and D)
PQ = 3233 <= modulus (give this to others)
E = 17    <= public exponent (give this to others)
D = 2753  <= private exponent (keep this secret!)

Your public key is (E,PQ).
Your private key is D.
```

The encryption function is: $\text{encrypt}(T) = (T^E) \bmod PQ$
 $= (T^{17}) \bmod 3233$

The decryption function is: $\text{decrypt}(C) = (C^D) \bmod PQ$
 $= (C^{2753}) \bmod 3233$

To encrypt the plaintext value 123, do this:

```
encrypt(123) = (123^17) mod 3233
                = 337587917446653715596592958817679803 mod 3233
                = 855
```

To decrypt the cipher text value 855, do this:

```
decrypt(855) = (855*2753) mod 3233
                = 123
```



Message Digest (One-way Hash) Functions



Document



Message Digest Function

a14092af948b938569584e5b8d8d307a

Hash Value

Hash functions **calculate a unique fixed-size bit string** representation called a message digest of any arbitrary block of information



If any given bit of the function's input is changed, every output bit has a **50 percent** chance of changing



It is computationally infeasible to have two files with the **same message digest value**



Note: Message digests are also called one-way hash functions because they cannot be reversed



Message Digest Function: MD5



MD5 Algorithm



MD5 algorithm takes a message of arbitrary length as input and outputs a 128-bit fingerprint or message digest of the input

MD5 hash is a 32-digit hexadecimal number

MD5 is not collision resistant, use of latest algorithms such as SHA-2 and SHA-3 is recommended

It is still deployed for digital signature applications, file integrity checking and storing passwords



<http://www.bitdreamers.com>



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Secure Hashing Algorithm (SHA)



It is an algorithm for generating cryptographically secure one-way hash, published by the **National Institute of Standards and Technology** as a **U.S. Federal Information Processing Standard**

SHA1

It produces a **160-bit digest** from a message with a maximum length of **(2⁶⁴ – 1) bits**, and resembles the MD5 algorithm

SHA2

It is a family of two similar hash functions, with different block sizes, namely **SHA-256** that uses **32-bit words** and **SHA-512** that uses **64-bit words**

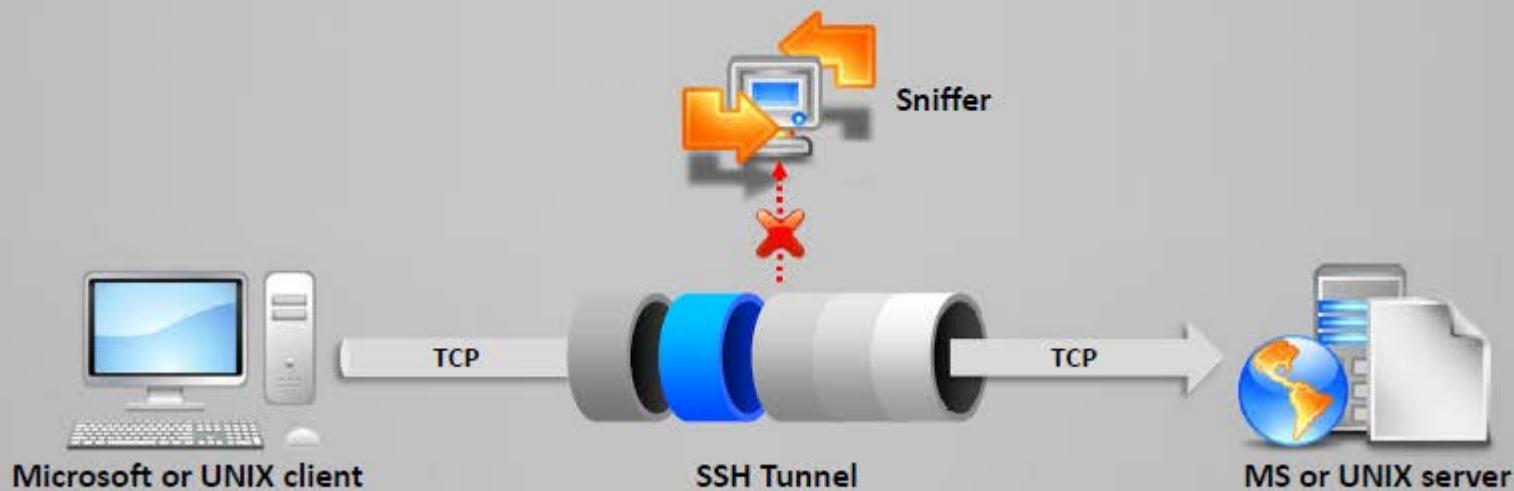
SHA3

SHA-3 uses the **sponge construction** in which message blocks are **XORed** into the initial bits of the state, which is then invertibly permuted

What is SSH (Secure Shell)?



- 1 SSH is a secure replacement for **telnet** and the **Berkeley remote-utilities** (rlogin, rsh, rcp, and rdist)
- 2 It provides an **encrypted channel** for remote logging, command execution and file transfers
- 3 Provides strong **host-to-host and user authentication**, and secure communication over an insecure Internet



Note: SSH2 is a more secure, efficient, and portable version of SSH that includes SFTP, an SSH2 tunneled FTP

Module Flow



1
Cryptography Concepts

2
Encryption Algorithms

3
Cryptography Tools

4
Public Key Infrastructure (PKI)

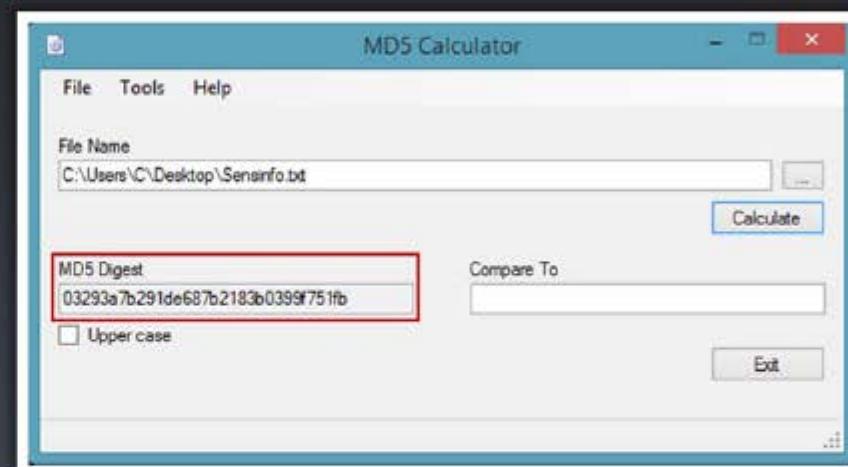
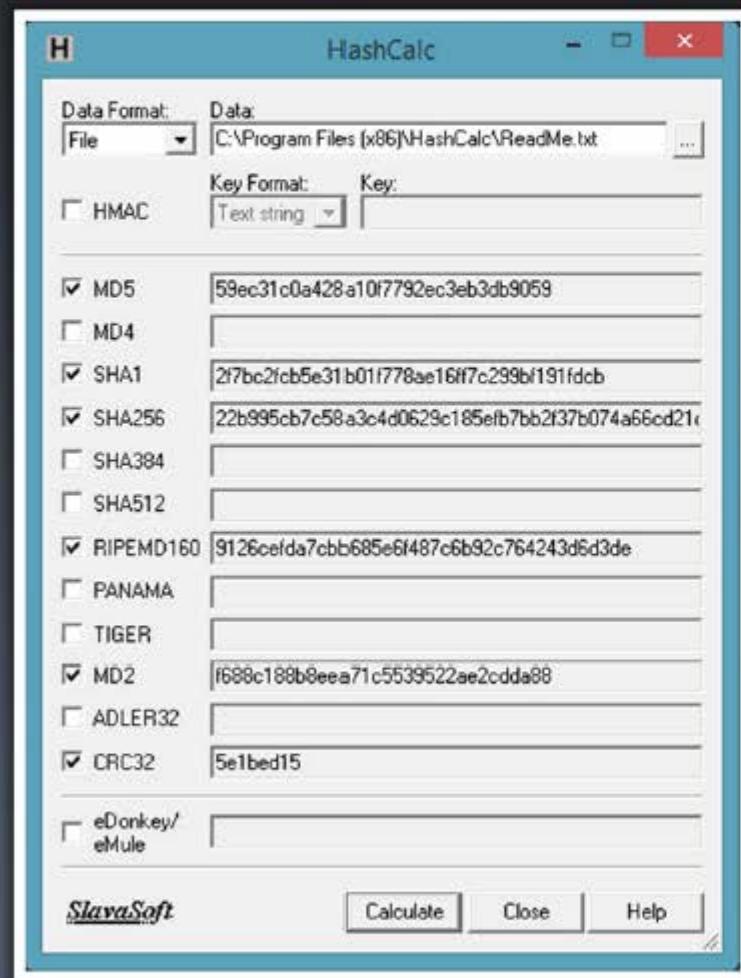
5
Email Encryption

6
Disk Encryption

7
Cryptography Attacks

8
Cryptanalysis Tools

MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles


<http://www.bullzip.com>

File	MD5	SHA1	CRC32	SHA-256	SHA-512	SHA-384
Sensinfo.txt	03293a7b291de687b21...	8eb1fcfa37ff35fb...	6ea774af	6b06ca5b370a77...	6d85e01b0e0dc4837...	ac1d73496a8313...
Carrier File.txt	17fe4eab4273e205e51...	0515344fc2e6860...	dbbf4f87	c080af7927702f42...	4020c05b2aef7b1...	ad17b0a7e76267...
Business Plan.docx	196c7957c0b7184424d...	707d1450f6a399...	89406083	91a1d22030569f98...	dec5429a424a192...	73d62c7e70fc4d...
Pwd List.docx	27b66cc87d1702a11b...	c48cf2b22cea1...	ecf58913	55c504eb7571f...	824d18d59271f...	cdd49108e194e...
Test Hashes.txt	2483a3be7296bc800c49...	94da559d019e0d...	ffcac573	647b126a0fb733...	92b56444bd93c...	326137de32701c...
irc.log	f6e51c00991a70c654...	58471ba6fa0a0...	527c65b1	413ba5c155ca59...	7a5e7c616a702b1...	70220da5a3d0...
Win7x64-windows...	18829fb571532d913...	05c7cb9a1c032a1...	30196325	e9c0960c242ff103...	057090aa9971689e2...	4a9071da594d0ed...

File(s), 1 Selected

Nirsoft Freeware. <http://www.nirsoft.net>

<http://www.nirsoft.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hash Calculators for Mobile: MD5 Hash Calculator, Hash Droid, and Hash Calculator



MD5 Hash Calculator



Hash Droid



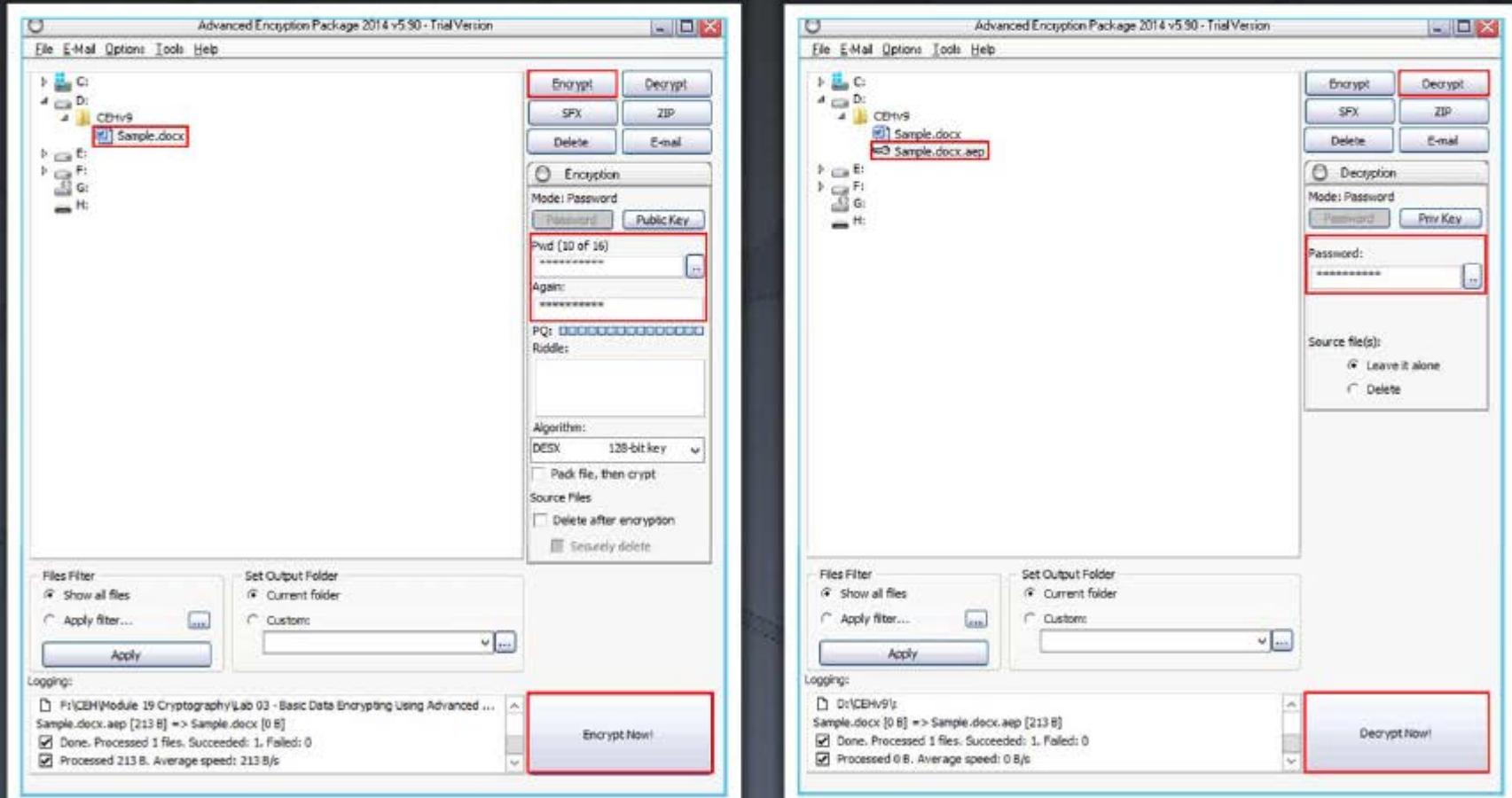
Hash Calculator



Cryptography Tool: Advanced Encryption Package 2014

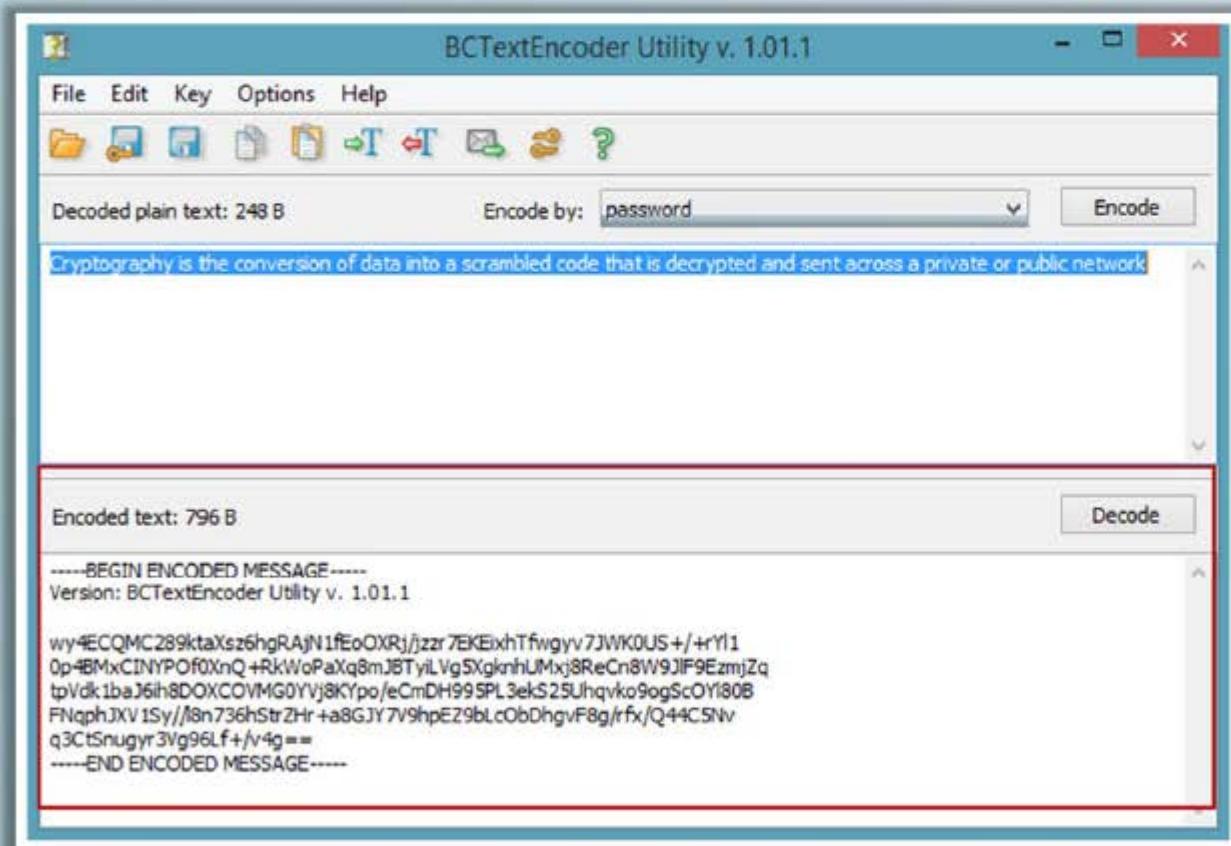


- Advanced Encryption Package 2014 file encryption software supports **symmetric and asymmetric encryption**


<http://www.aeppro.com>

Copyright © by EC-COUNCIL. All Rights Reserved. Reproduction is Strictly Prohibited.

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>**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.littleelite.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

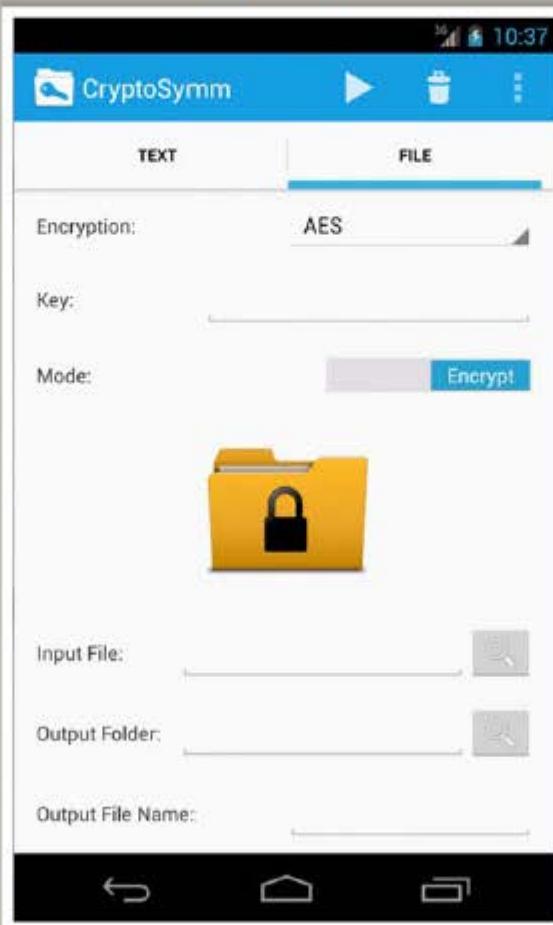


Secret Space Encryptor



<http://www.paranoiaworks.mobi>

CryptoSymm



<https://play.google.com>

Cipher Sender



<https://play.google.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow



1

Cryptography Concepts

2

Encryption Algorithms

3

Cryptography Tools

4

Public Key Infrastructure (PKI)

5

Email Encryption

6

Disk Encryption

7

Cryptography Attacks

8

Cryptanalysis Tools

Public Key Infrastructure (PKI)



Public Key Infrastructure (PKI) is a **set of hardware, software, people, policies, and procedures** required to create, manage, distribute, use, store, and revoke **digital certificates**

Components of PKI

1 Certificate Management System

Generates, distributes, stores, and verifies certificates

2 Digital Certificates

Establishes credentials of a person when doing online transactions

3 Validation Authority (VA)

Stores certificates (with their public keys)

4 Certificate Authority (CA)

Issues and verifies digital certificates

5 End User

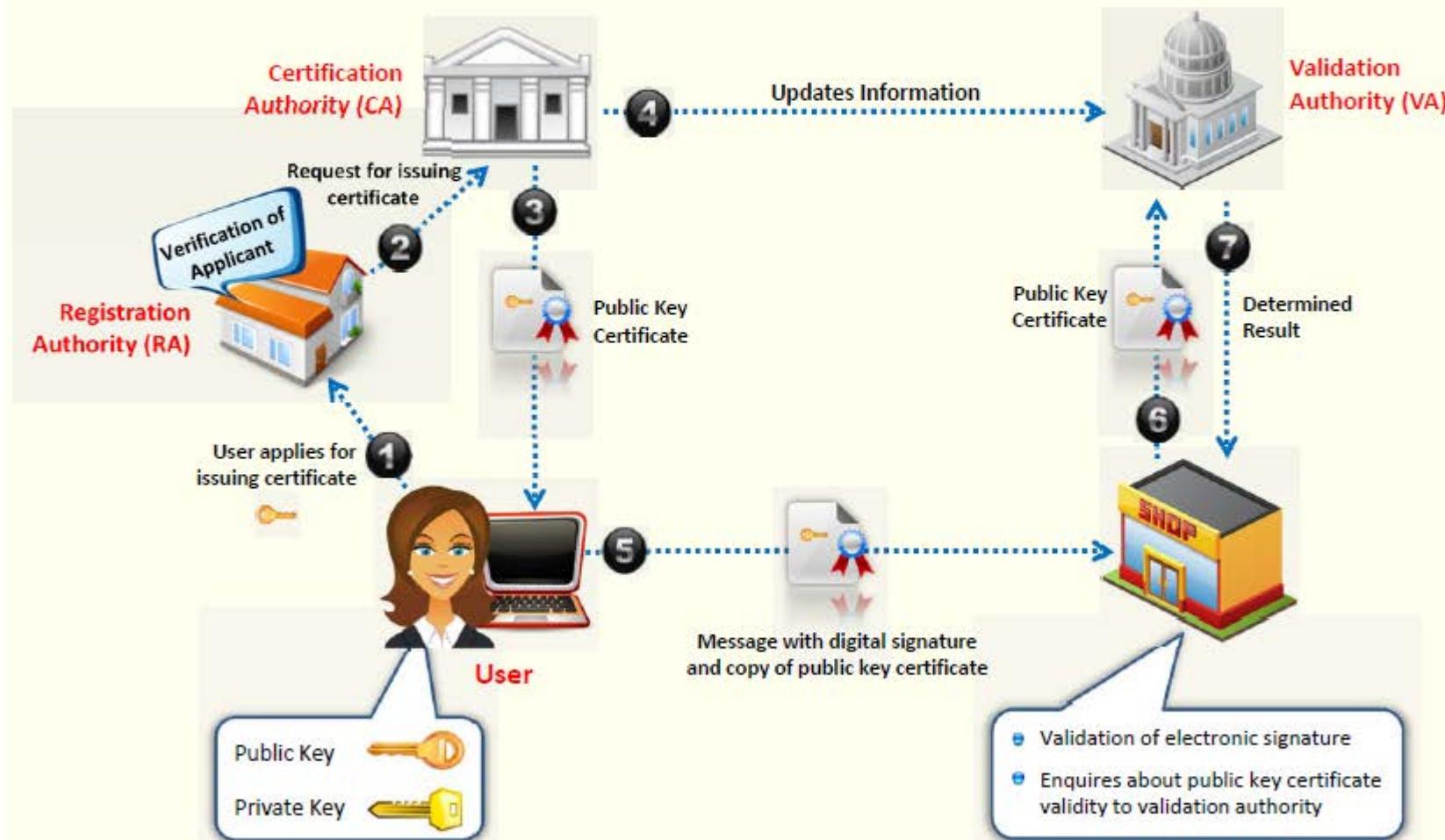
Requests, manages, and uses certificates

6 Registration Authority (RA)

Acts as the verifier for the certificate authority

Public Key Infrastructure (PKI)

(Cont'd)



Certification Authorities



COMODO
Creating Trust Online®

Products Home & Office Business E-Commerce Business & Enterprise Partners Social Media

The First To Bring You a Full Line of 2048-bit Certificates

Comodo brings you next generation compliance today with our line of 2048-bit SSL.

Explore Our SSL Certificates

- Email Server
- Server & Website
- Apache Domains
- IIS Certificate 2007™
- Secure Mail Server
- SSL Certificate

[SHOP CERTIFICATES](#)

[View All Certificates](#)

FREE PRODUCTS MORE COMPUTING BUSINESS SOLUTIONS E-COMMERCE SOLUTIONS ENTERPRISE SOLUTIONS

<http://www.comodo.com>

Contact Us • 1-888-484-2063 Chat sales@thawte.com Change Details

thawte Products Partners Support Resources My Account SEARCH

The most visible sign of web site security

Show your customers your site is safe with Extended Validation SSL.

[Learn more](#)

Buy Certificates White Paper Manage Multiple Certificates Not all SSL is the Same

[Buy SSL Certificate](#) [Buy Code Signing](#) [Understanding SSL Certificates](#) [WPS Paper](#) [Manage certificates across any size organization with ease!](#) [Compare Thawte to other SSL providers and see the difference!](#)

<http://www.thawte.com>

Assured by Symantec VeriSign Authentication Services

United States (Change) Contact Symantec Norton Security

Products & Services Partners Support My Account

Norton SECURED powered by VeriSign

Same check. New name. Still the gold standard.

The same security, services and support you've come to trust from VeriSign are now brought to you by Symantec.

What it means for you:

- BUY SSL Certificates
- BUY Symantec™ Safe Site
- BUY Code Signing
- TRY Free Trial
- REVIEW Review SSL Certificates
- SIGN IN Trust Center
- Norton™ Secured Seal

Trust from Search to Browser to Buy

Boost your site traffic and conversions with powerful trial features. Free with every SSL Certificate.

Protect Your Site. Grow Your Business.

New features from Symantec SSL make your Web site easy to trust and easy to secure.

VERISHIELD™

Cyber security and availability products your business relies on.

- Managed DNS
- DDoS Protection
- ICIDefer™
- Domain Name Services

are available from VeriSign at [VeriSign.com](#)

<http://www.symantec.com>

United States (Change) Contact Entrust

SECURITY ON:SSL Entrust Discovery

Find, inventory and manage ALL certificates across ALL your systems and environments

> Why Entrust > Products > Support > Partners > About Us > My Account

Phone Blog Email

Go Wild! New Wildcard SSL Certificates from \$725/year

EV Multi-Domain SSL Certificates from \$373/year

ICG Multi-Domain SSL Certificates from \$249/year

Advantage SSL Certificates from \$186/year

Apple iOS Device Certificates from \$155/year

<http://www.entrust.net>

Signed Certificate (CA) Vs. Self Signed Certificate



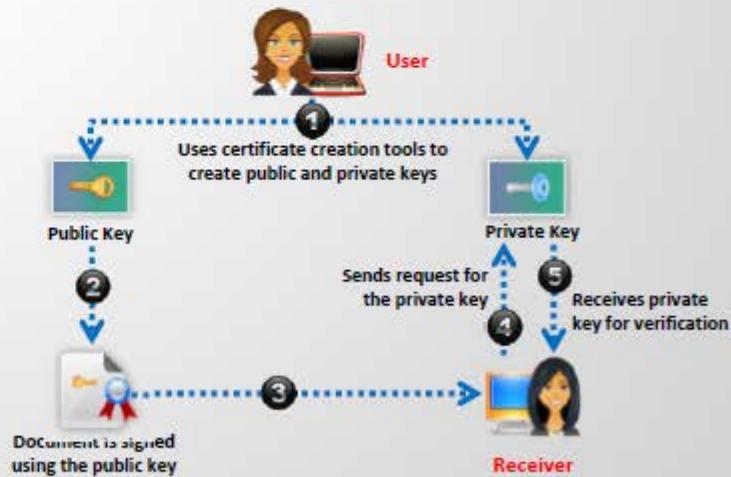
Signed Certificate

- User approaches a trustworthy **Certification Authority (CA)** and purchases digital certificate
- User gets the **public key** from the CA, he signs the document using it
- The signed document is delivered to the receiver
- The receiver can verify the certificate by enquiring in **Validation Authority (VA)**
- VA verifies the certificate to the receiver but it does not share private key



Self-signed Certificate

- User creates public and private keys using a tool such as **Adobe Reader**, **Java's keytool**, **Apple's Keychain**, etc.
- User uses public key to **sign the document**
- The **self-signed document** is delivered to the receiver
- The receiver request the user for his **private key**
- User **shares the private key** with the receiver



Module Flow



1

Cryptography Concepts

2

Encryption Algorithms

3

Cryptography Tools

4

Public Key Infrastructure (PKI)

5

Email Encryption

6

Disk Encryption

7

Cryptography Attacks

8

Cryptanalysis Tools

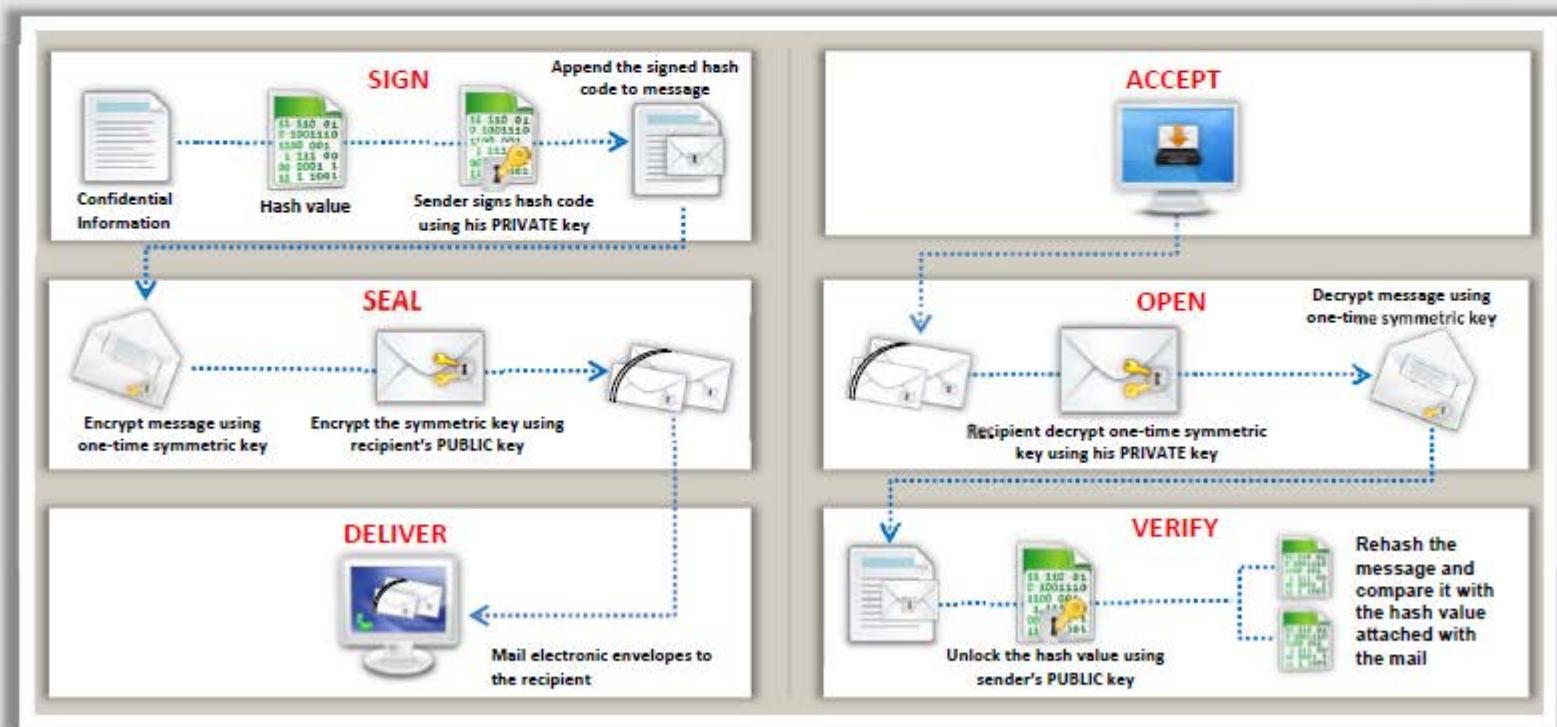
Digital Signature



1
2

Digital signature used asymmetric cryptography to simulate the security properties of a **signature in digital, rather than written form**

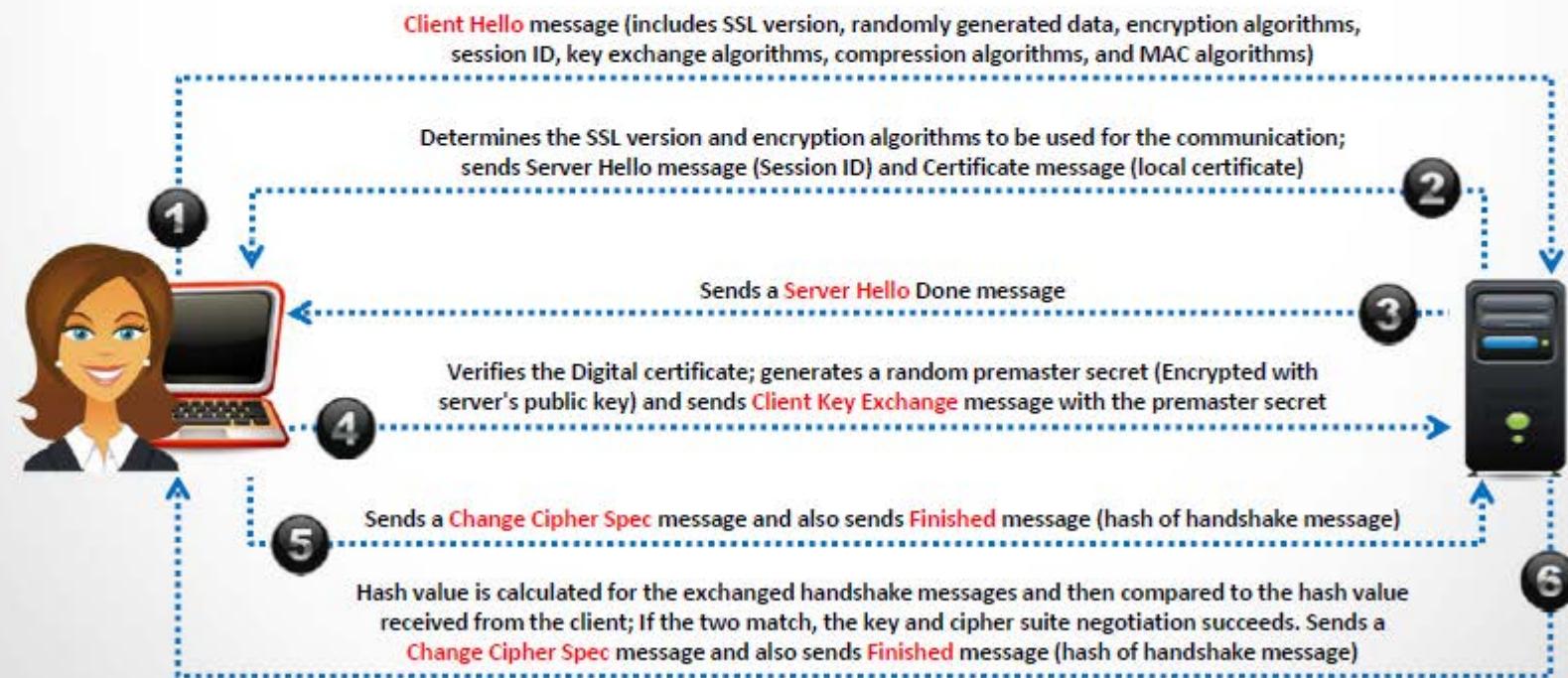
A digital signature may be further protected, by **encrypting the signed email** for confidentiality



SSL (Secure Sockets Layer)



- SSL is an application layer protocol developed by Netscape for **managing the security** of a message transmission on the Internet
- It uses **RSA asymmetric (public key) encryption** to encrypt data transferred over SSL connections



Transport Layer Security (TLS)



- TLS is a protocol **to establish a secure connection** between a client and a server and ensure privacy and integrity of information during transmission
- It uses the RSA algorithm with 1024 and 2048 bit strengths

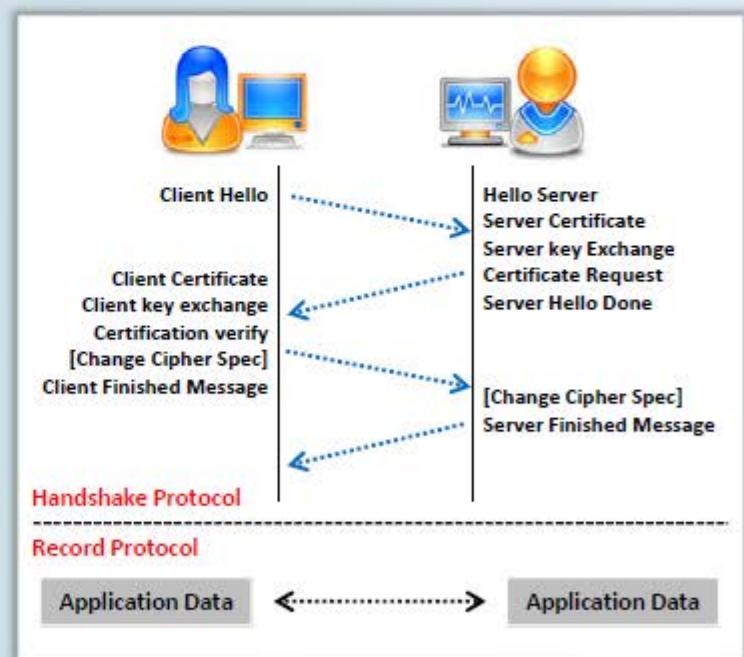


TLS Handshake Protocol

It allows the client and server to authenticate each other, select encryption algorithm, and exchange symmetric key prior to data exchange

TLS Record Protocol

It provides secured connections with an encryption method such as Data Encryption Standard (DES)



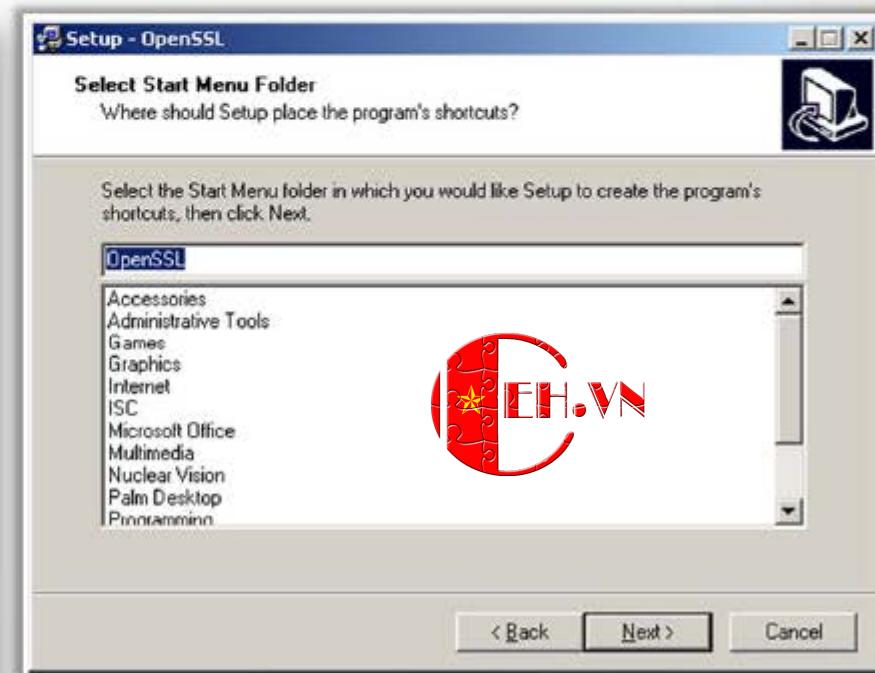
Cryptography Toolkit: OpenSSL



- OpenSSL is an open source cryptography toolkit implementing the **Secure Sockets Layer (SSL v2/v3)** and **Transport Layer Security (TLS v1)** network protocols and related cryptography standards required by them
- The openssl program is a command line tool for using the various **cryptography functions** of OpenSSL's crypto library from the shell

OpenSSL can be used for:

- Creation and management of private keys, public keys and parameters
- Public key cryptographic operations
- Creation of X.509 certificates, CSRs and CRLs
- Calculation of Message Digests
- Encryption and Decryption with Ciphers
- SSL/TLS Client and Server Tests
- Handling of S/MIME signed or encrypted mail
- Time Stamp requests, generation and verification



<https://www.openssl.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cryptography Toolkit: Keyczar



- Keyczar is an open source cryptographic toolkit designed to make it easier and safer for developers to use **cryptography in their applications**
- It **supports authentication** and **encryption** with both symmetric and asymmetric keys

<http://www.keyczar.org>



Features

- Key rotation and versioning
- Safe default algorithms, modes, and key lengths
- Automated generation of initialization vectors and ciphertext signatures
- Java, Python, and C++ implementations
- International support in Java

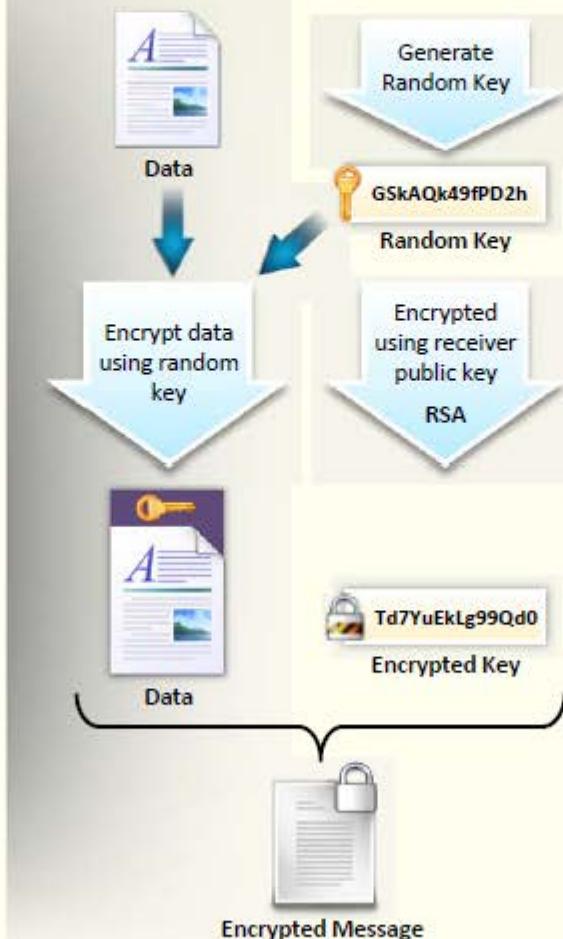
Pretty Good Privacy (PGP)



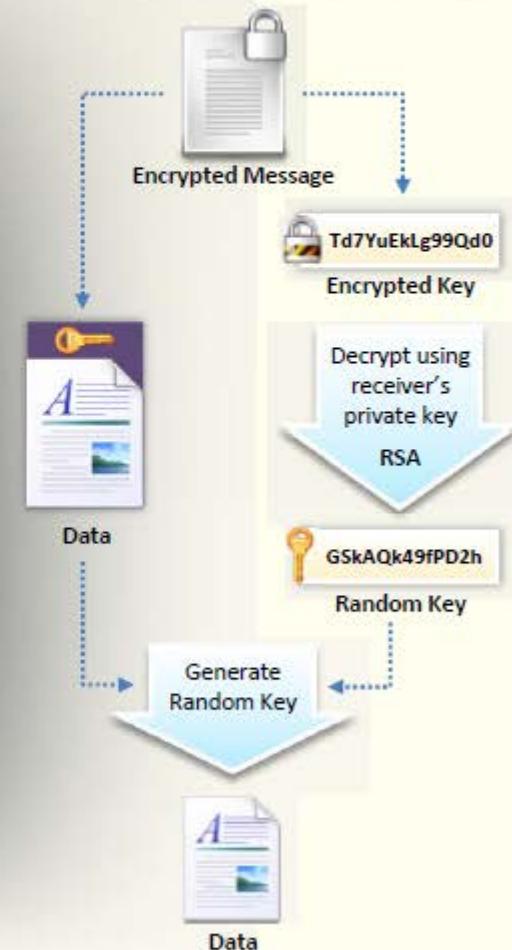
Pretty Good Privacy

- PGP (Pretty Good Privacy) is a protocol used to **encrypt** and **decrypt** data that provides **authentication** and **cryptographic privacy**
- PGP is often used for data **compression**, **digital signing**, encryption and decryption of **messages**, **emails**, **files**, **directories**, and to enhance privacy of email communications
- PGP combines the best features of both **conventional** and **public key cryptography** and is therefore known as **hybrid cryptosystem**

PGP Encryption



PGP Decryption



Module Flow



1

Cryptography Concepts

2

Encryption Algorithms

3

Cryptography Tools

4

Public Key Infrastructure (PKI)

5

Email Encryption

6

Disk Encryption

7

Cryptography Attacks

8

Cryptanalysis Tools

Disk Encryption



01

Confidentiality



Disk encryption protects **confidentiality of the data** stored on disk by converting it into an unreadable code using disk encryption software or hardware

- Privacy
- Passphrase
- Hidden Volumes

02

Encryption



Disk encryption works in a similar way as **text message encryption** and protects data even when the OS not active

- Volume Encryption

03

Protection



With the use of an encryption program for your disk, you can **safeguard any information** to burn onto the disk, and keep it from falling into the wrong hands

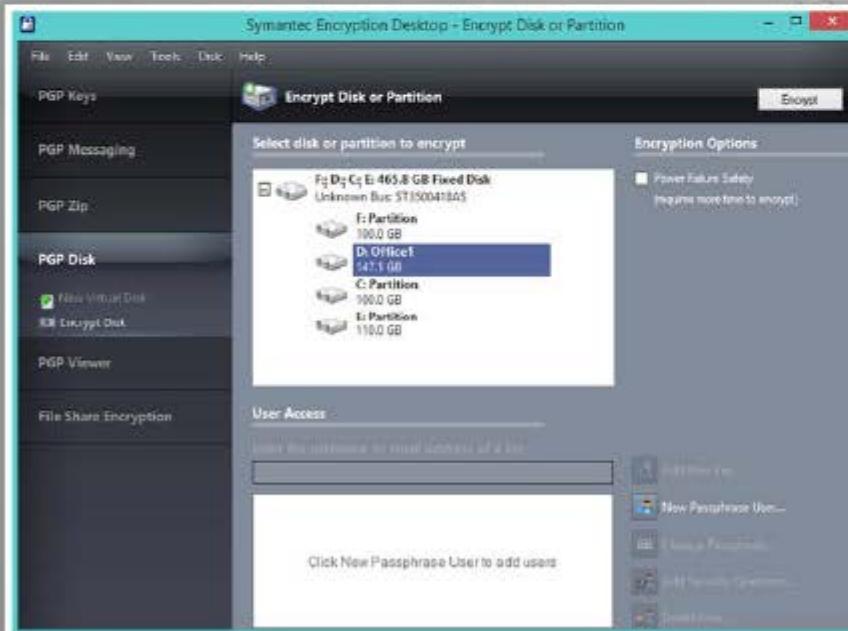
- Blue Ray
- DVD
- Backup

Disk Encryption Tools: Symantec Drive Encryption and GiliSoft Full Disk Encryption



Symantec Drive Encryption

- Symantec Drive Encryption provides **full disk encryption** for all data (user files, swap files, system files, hidden files, etc.) on desktops, laptops, and removable media
- It protects data from **unauthorized access**



<http://www.symantec.com>

GiliSoft Full Disk Encryption

- GiliSoft Full Disk Encryption offers encryption of all **disk partitions**, including the system partition
- It **provides automatic security** for all information on endpoint hard drives, including user data, operating system files and temporary and erased files



<http://www.gilisoft.com>

Disk Encryption Tools



DriveCrypt
<http://www.securstar.com>



ShareCrypt
<http://www.securstar.com>



PocketCrypt
<http://www.securstar.com>



Rohos Disk Encryption
<http://www.rohos.com>



R-Crypto
<http://www.r-tt.com>



east-tec SafeBit
<http://www.east-tec.com>



DiskCryptor
<http://diskcryptor.net>



alertsec
<http://www.alertsec.com>



Cryptainer LE
<http://www.cypherix.com>



DriveCrypt Plus Pack
<http://www.securstar.com>

Module Flow



1
Cryptography Concepts

2
Encryption Algorithms

3
Cryptography Tools

4
Public Key Infrastructure (PKI)

5
Email Encryption

6
Disk Encryption

7
Cryptography Attacks

8
Cryptanalysis Tools

Cryptography Attacks



- Cryptography attacks are based on the assumption that the cryptanalyst has access to the **encrypted information**



Ciphertext-only attack



Known-plaintext attack



Chosen-plaintext



Chosen - ciphertext attack



Chosen-key attack



Adaptive chosen-plaintext attack



Timing attack



Rubber hose attack

Cryptography Attacks

(Cont'd)



Ciphertext-only Attack

Attacker has access to the cipher text; goal of this attack to **recover encryption key** from the ciphertext

Adaptive Chosen-plaintext Attack

Attacker makes a **series of interactive queries**, choosing subsequent plaintexts based on the information from the previous encryptions

Chosen-plaintext Attack

Attacker **defines his own plaintext**, feeds it into the cipher, and analyzes the resulting ciphertext

Known-plaintext Attack

Attacker has **knowledge of some part of the plain text**; using this information the key used to generate ciphertext is deduced so as to decipher other messages

Cryptography Attacks

(Cont'd)



Chosen-ciphertext Attack

Attacker obtains the plaintexts corresponding to an **arbitrary set** of ciphertexts of his own choosing



Extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by **coercion or torture**

Rubber Hose Attack

Chosen-key Attack

A **generalization** of the chosen-text attack



It is based on repeatedly measuring the **exact execution times** of modular exponentiation operations

Timing Attack

Code Breaking Methodologies



Trickery and Deceit

It involves the use of **social engineering techniques** to extract cryptography keys



Brute-Force

Cryptography keys are discovered by **trying every possible combination**



One-Time Pad

A one-time pad contains many **non-repeating groups of letters** or number keys, which are chosen randomly



Frequency Analysis

- It is the study of the frequency of letters or groups of letters in a **ciphertext**
- It works on the fact that, in any given stretch of written language, certain letters and **combinations of letters** occur with varying frequencies



Brute-Force Attack



Attack Scheme

Defeating a cryptographic scheme by **trying a large number of possible keys** until the correct encryption key is discovered



Brute-Force Attack

Brute-force attack is a **high resource and time intensive process**, however, more certain to achieve results



Success Factors

Success of brute force attack depends on **length of the key, time constraint, and system security mechanisms**

Power/Cost	40 bits (5 char)	56 bit (7 char)	64 bit (8 char)	128 bit (16 char)
\$ 2K (1 PC. Can be achieved by an individual)	1.4 min	73 days	50 years	10^{20} years
\$ 100K (this can be achieved by a company)	2 sec	35 hours	1 year	10^{19} years
\$ 1M (Achieved by a huge organization or a state)	0.2 sec	3.5 hours	37 days	10^{18} years

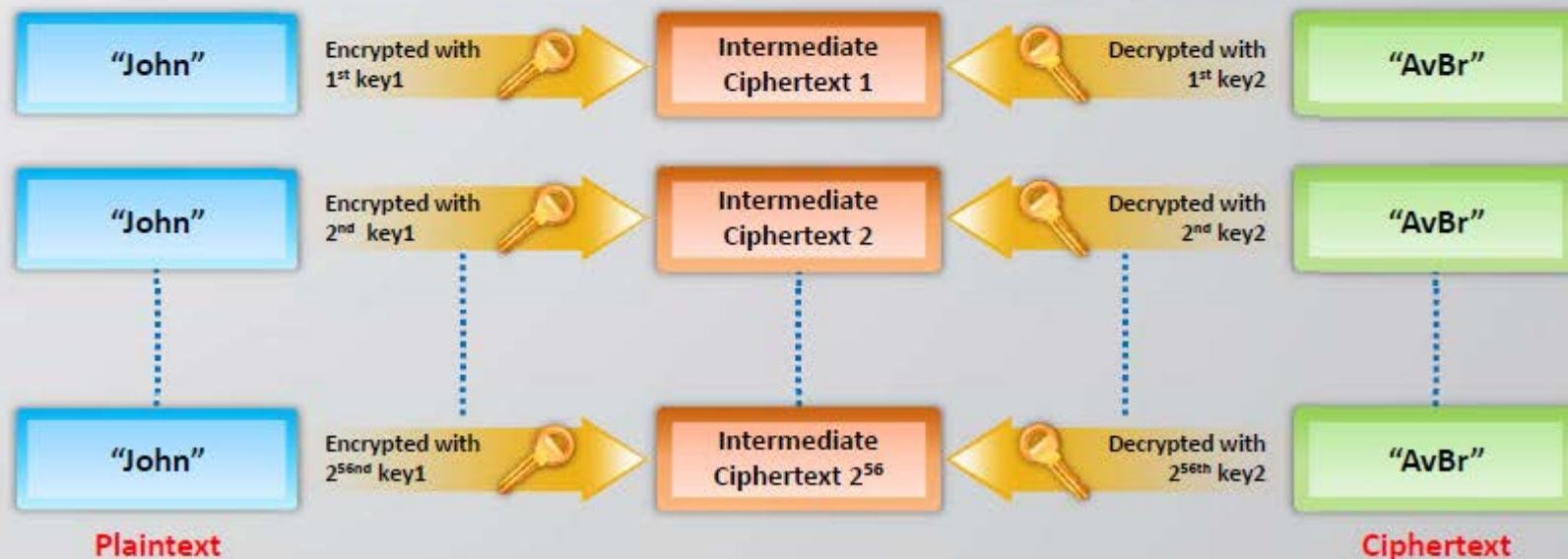
Estimate Time for Successful Brute-force Attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Meet-in-the-Middle Attack on Digital Signature Schemes



- The attack works by **encrypting from one end** and **decrypting from the other end**, thus meeting in the middle
- It can be used for **forging signatures** even on digital signatures that use multiple-encryption scheme



Side Channel Attack

**01**

Side channel attack is a **physical attack** performed on a cryptographic device/ cryptosystem to gain sensitive information

02

Cryptography is generally **implemented in hardware or software** which runs on physical devices such as semi-conductors

03

These semi-conductor devices include **resistor, transistor** and so on

04

These physical devices are affected by various **environmental factors** that include: power consumption, electro-magnetic field, light emission, timing and delay, and sound

05

In Side Channel attack, an attacker **monitors these channels (environmental factors)** and try to acquire the information useful for cryptanalysis

06

The information collected in this process is termed as **side channel information**

07

Side Channel Attacks (SCA) are **no way related to traditional/ theoretical form of attacks** like brute force attack

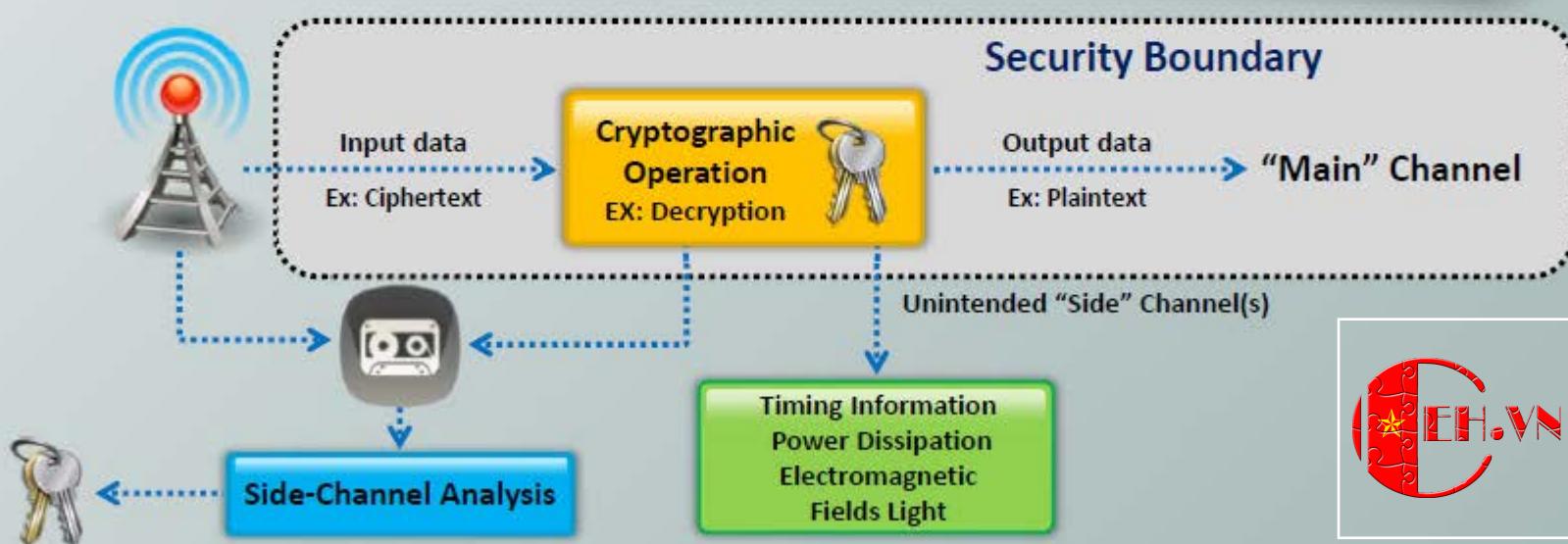
08

The concept of SCA is **based on the way, the cryptographic algorithms are implemented**, rather than at the algorithm itself

Side Channel Attack - Scenario



- Assume that an encrypted data is to be decrypted and displayed a plain text, inside a **trusted zone**
- At the time of decryption in a cryptosystem, **physical environmental factors** such as timing, power dissipation etc., acting on the components of a computer are recorded by an attacker
- The attacker analyzes this information in an attempt **to gain useful information** for cryptanalysis



Module Flow



1

Cryptography Concepts

2

Encryption Algorithms

3

Cryptography Tools

4

Public Key Infrastructure (PKI)

5

Email Encryption

6

Disk Encryption

7

Cryptography Attacks

8

Cryptanalysis Tools



CrypTool 1.4.31 Beta 6b [VS2008] - Unnamed1

- File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
- Encrypt/Decrypt
 - Symmetric (classic)
 - Symmetric (modern)
 - RC2...
 - Asymmetric
 - Hybrid
- Digital Signatures/PKI
- Indiv. Procedures
- Analysis
- Options
- Window
- Help

CrypTool 1 is a free e-learning program in the area of cryptography and cryptanalysis offering extensive visualizations.

Encryption / decryption with RC2 L:1 C:154 P:154

<http://www.cryptool.org>

RC2 encryption of <Unnamed1>, key <00>

Hex	Dec	Text
00000000	76 F5 D1 14	F2 13 00 99 6A 61 CB 2D v.....ja.-
0000000C	0A 31 5C 85	91 84 7F 19 97 C2 12 03 1\.....tb.....n.
00000018	A4 D0 E8 74	62 DF 10 18 FA C8 6D 09 2=rN.....Tn.
00000024	A4 5E 18 A7	E4 FB B0 05 0F 69 C2 29 H }=0.....D[
00000030	20 32 3D 72	4E DE 12 B1 54 6D 80 .+..y.2..
0000003C	CE 48 C6 7D	73 30 F1 F8 9F 44 A0 5B f.....I..
00000048	EF 8D 0B 2B	E5 D0 3A 79 81 32 92 AD 1....u).....(E]
00000054	3A 1A 66 D2	D6 A7 06 94 2C 49 96 92 ?..V@.p.?..
00000060	6C 1C 8A CC	C9 75 29 A9 F7 F2 C6 F8 <.e.HX...Q<.....
0000006C	2E 0E C0 A0	15 28 D7 45 1D EB 19 5D
00000078	3F D7 C5 56	40 0F 70 F4 F2 3F 02 B9
00000084	FC 69 E8 DB	FB 64 C8 96 90 F2 00 10
00000090	3C ED 65 D2	48 58 CE F9 C2 51 3C BE
0000009C	92 85 87 8B

■ CrypTool is a free e-learning program in the area of **cryptography** and **cryptoanalysis**

- Subprojects of CrypTool:
- CrypTool 1 (CT1)
 - CrypTool 2 (CT2)
 - JCrypTool (JCT)
 - CrypTool-Online (CTO)

Cryptanalysis Tools



CryptoBench
<http://www.addario.org>



Jipher
<http://cipher.org.uk>



Ganzúa
<http://ganzua.sourceforge.net>



Crank
<http://crank.sourceforge.net>



EverCrack
<http://evercrack.sourceforge.net>



AlphaPeeler
<http://alphapeeler.sourceforge.net>



Draft Crypto Analyzer
<http://www.literatecode.com>



Linear Hull Cryptanalysis of PRESENT
<http://www.ecrypt.eu.org>



mediggo
<http://code.google.com>



SubCypher
<http://www.esclepiusllc.com>

Online MD5 Decryption Tools



MD5 Decrypt
<http://www.md5decrypt.org>

OnlineHashCrack.com
<http://www.onlinehashcrack.com>

MD5Cracker
<http://md5crack.com>

HashKiller.co.uk
<http://www.hashkiller.co.uk>

MD5 Decrypter
<http://www.md5online.org>

Md5.My-Addr.com
<http://md5.my-addr.com>

Hash Cracker
<http://www.hash-cracker.com>

cmd5.org
<http://www.cmd5.org>

MD5Decrypter
<http://www.md5decrypter.com>

CrackStation
<https://crackstation.net>

Module Summary



- ❑ Cryptography is the conversion of data into a scrambled code that is decrypted and sent across a private or public network
- ❑ Symmetric encryption uses the same key for encryption as it does for decryption and asymmetric encryption uses different encryption keys for encryption and decryption
- ❑ Ciphers are algorithms used to encrypt or decrypt the data
- ❑ Hash functions calculate a unique fixed-size bit string representation called a message digest of any arbitrary block of information
- ❑ Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates
- ❑ Digital signature used asymmetric cryptography to simulate the security properties of a signature in digital, rather than written form
- ❑ Disk encryption protects confidentiality of the data stored on disk by converting it into an unreadable code using disk encryption software or hardware
- ❑ Cryptography attacks are based on the assumption that the cryptanalyst has access to the encrypted information