Cryptography

Module 18

Engineered by Hackers. Presented by Professionals.

SECURITY NEWS

The Register®
Biting the hand that feeds IT

November 18, 2010 16:15 GMT

German 'hacker' uses rented computing to crack hashing algorithm
Brute force PAYG hack attack cracks SHA1 hashes – for $2

A German security enthusiast has used rented computing resources to crack a secure hashing algorithm (SHA-1) password.

Thomas Roth used a GPU-based rentable computer resource to run a brute force attack to crack SHA1 hashes. Encryption experts warned for at least five years SHA-1 could no longer be considered secure so what's noteworthy about Roth's project is not what he did or the approach he used, which was essentially based on trying every possible combination until he found a hit, but the technology he used.

SHA-1, although it is in the process of being phased out, still forms a component of various widely-used security applications, including Secure Sockets Layer, Transport Layer Security and S/MIME protocols. Roth claims to have cracked all the hashes from a 160-bit SHA-1 hash with a password of between one and six characters in around 49 minutes.

http://www.theregister.co.uk

CEH Certified Ethical Hacker

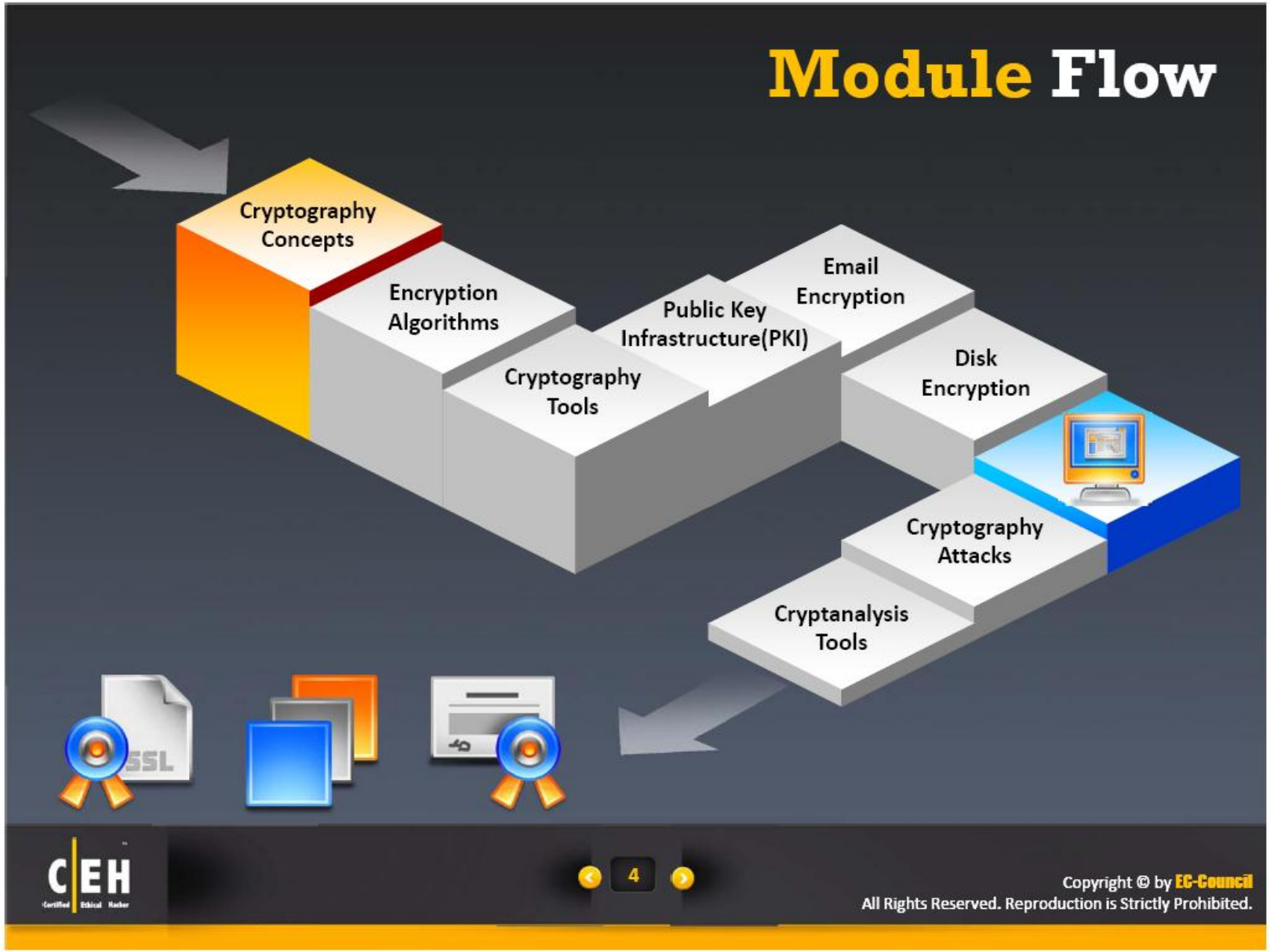
2

Module Objectives

- Cryptography
- Types of Cryptography
- Ciphers
- Advanced Encryption Standard (AES)
- RC4, RC5, RC6 Algorithms
- RSA (Rivest Shamir Adleman)
- Message Digest Function: MD5
- Secure Hashing Algorithm (SHA)

- Cryptography Tools
- Public Key Infrastructure (PKI)
- Digital Signature
- SSL (Secure Sockets Layer)
- Disk Encryption
- Disk Encryption Tools
- Cryptography Attacks
- Cryptanalysis Tools





Cryptography

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

Cryptography is used to protect e-mail messages, credit card information, and corporate data

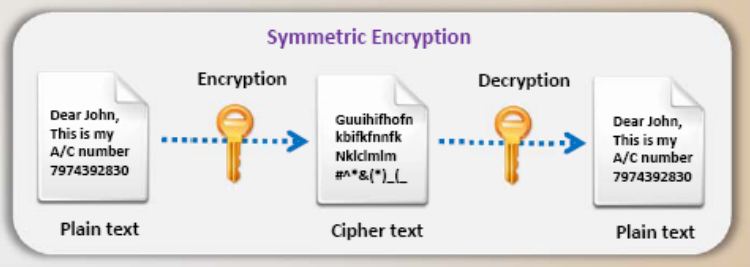
Objectives of Cryptography

1. Confidentiality
2. Integrity
3. Authentication
4. Non–Repudiation

Types of Cryptography

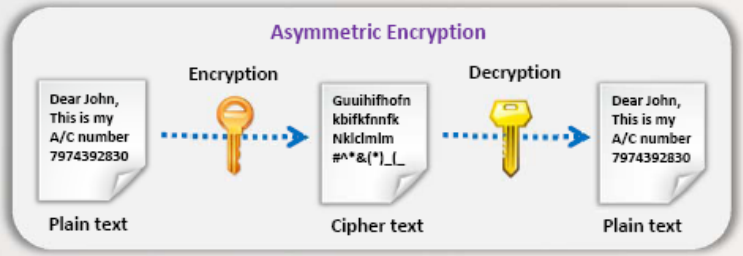
Symmetric Encryption

Symmetric encryption (secret-key, shared-key, and private-key) uses the same key for encryption as they do for decryption



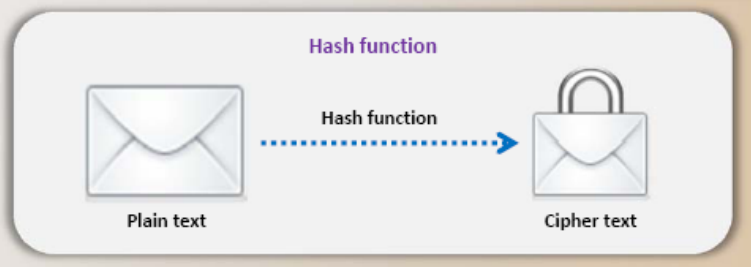
Asymmetric Encryption

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

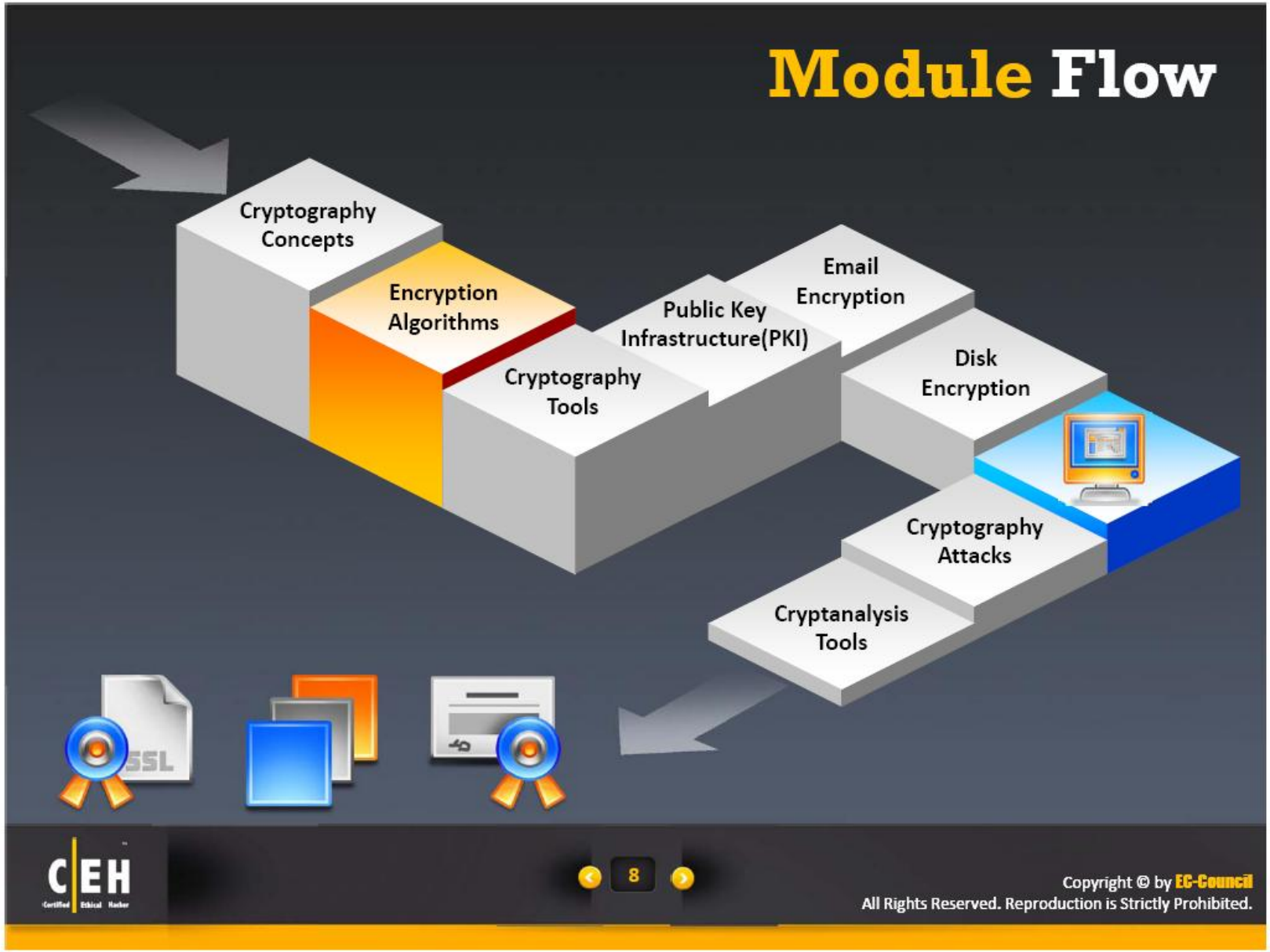


Hash Function

Hash function (message digests or one - way encryption) uses no key for encryption and decryption




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
CEH
7
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



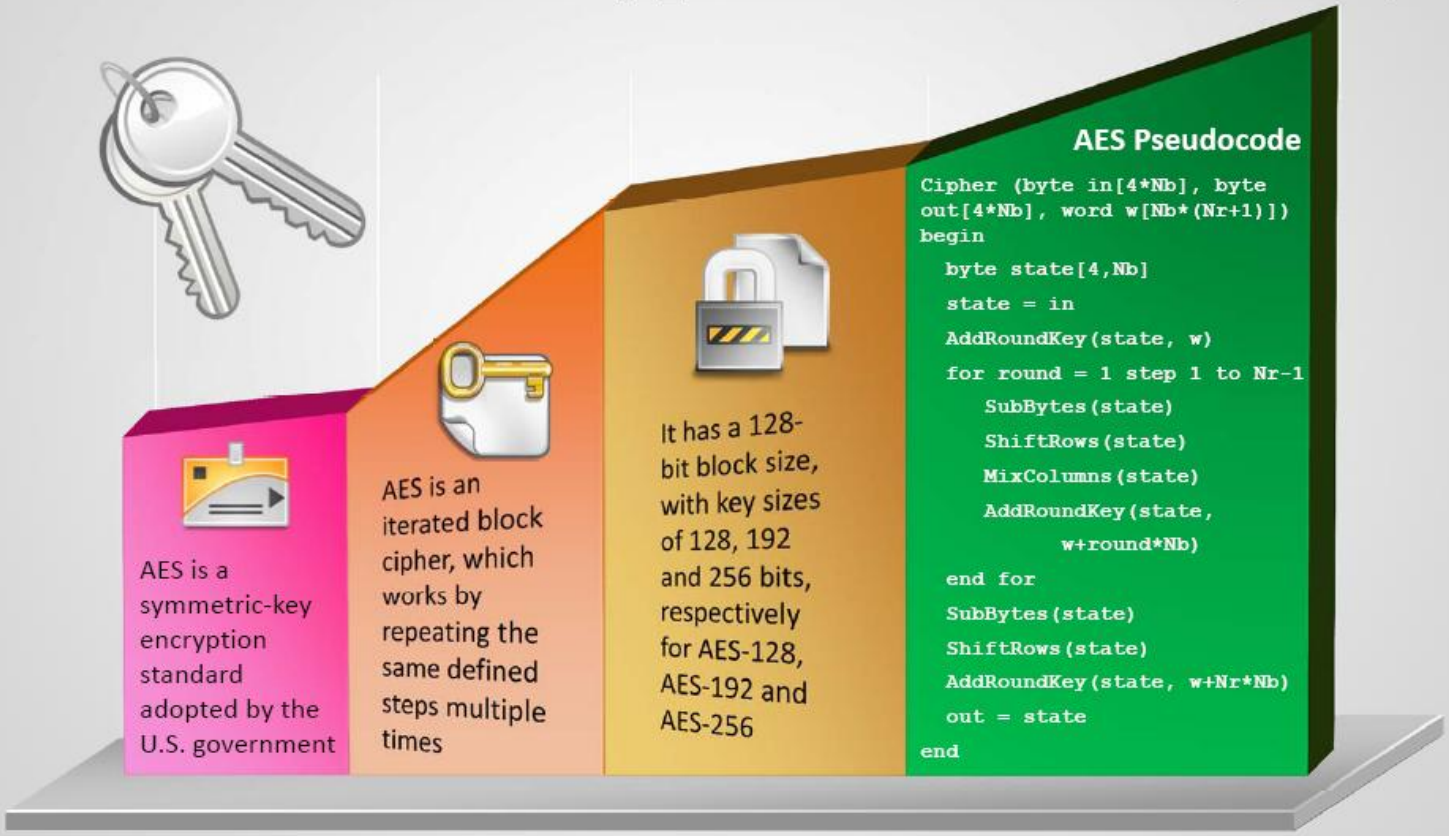
Ciphers

Ciphers are algorithms used to encrypt or decrypt the data

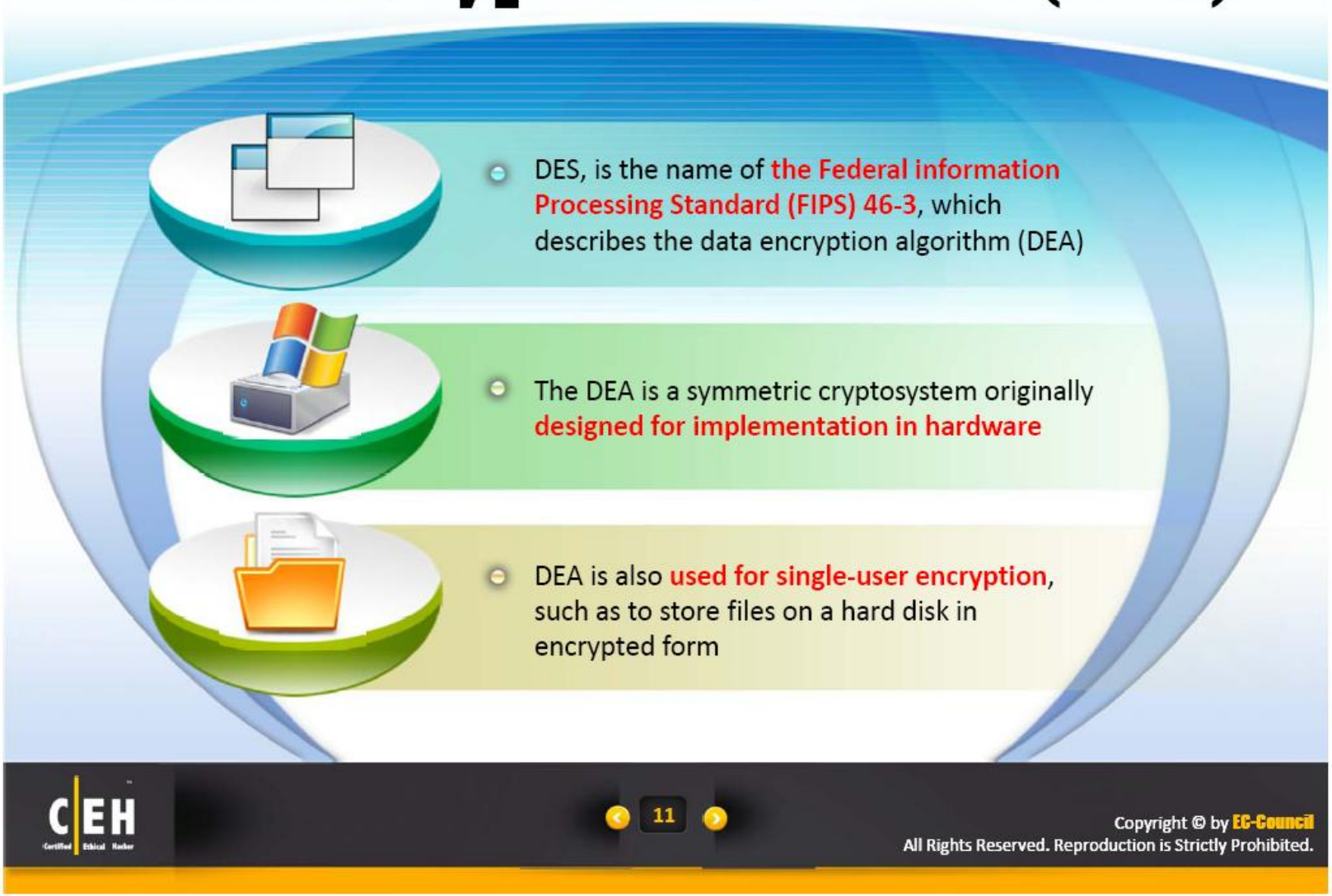
- **Classical Ciphers**
  - **Substitution cipher** — It replaces bits, characters, or blocks of characters with different bits, characters or blocks
  - **Transposition cipher** — The letters of the plaintext are shifted about to form the cryptogram
- **Modern Ciphers**

  - **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

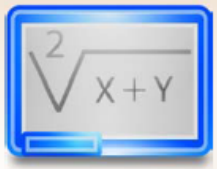
Advanced Encryption Standard (AES)



Data Encryption Standard (DES)



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

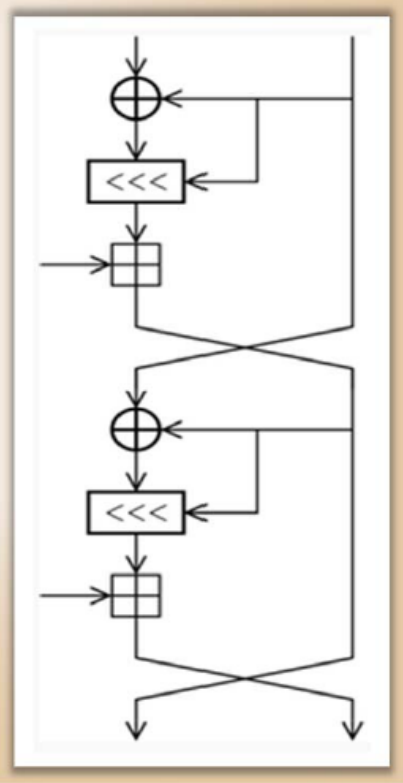
RC5

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 adds two features to RC5: the inclusion of integer multiplication, and the use of four 4-bit working registers instead of RC5's two 2-bit registers

RC5



The DSA and Related Signature Schemes

Digital Signature Algorithm

The DSA has become a U.S. Federal Information Processing Standard (FIPS 186) called the Digital Signature Standard (DSS)

Digital Signature

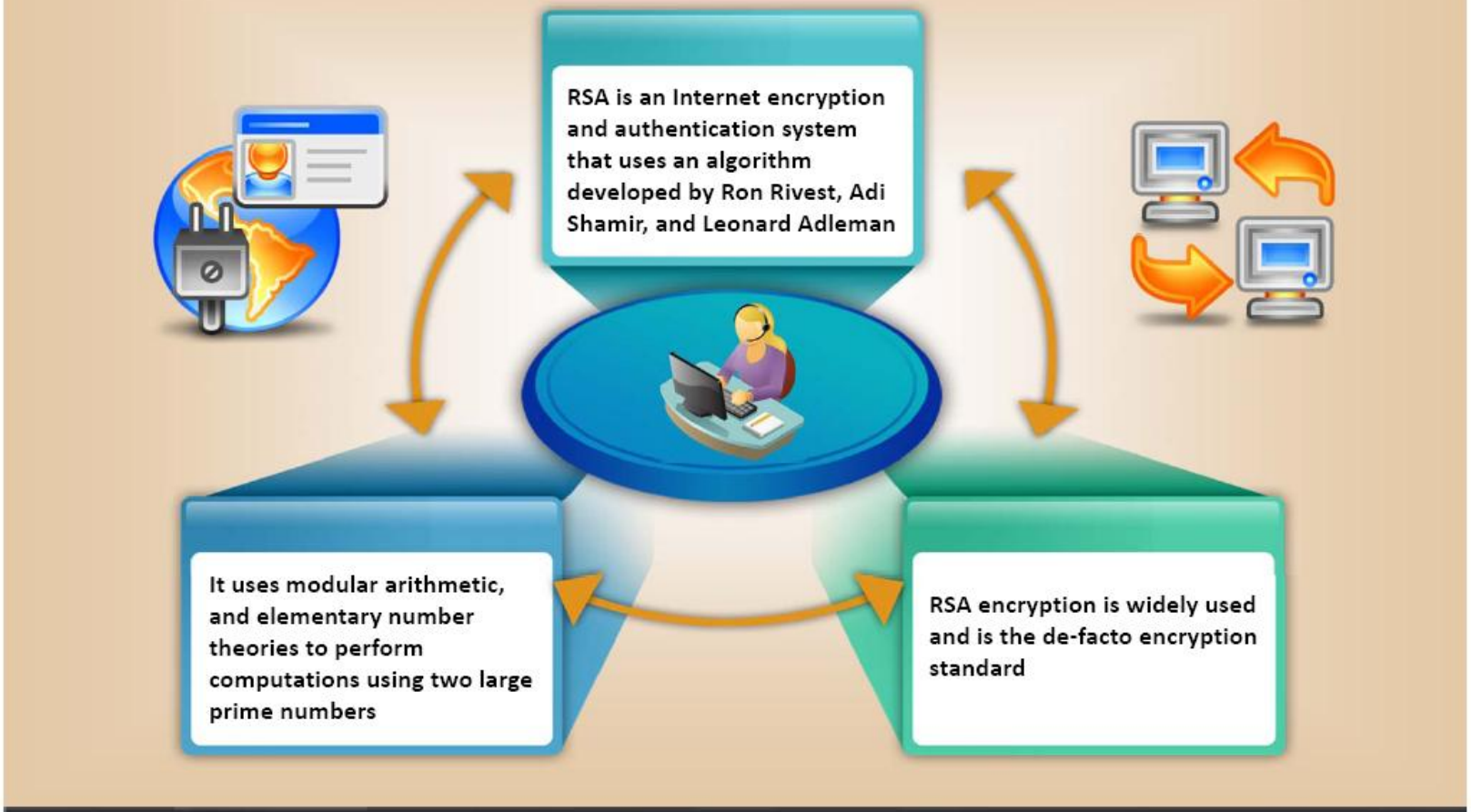
It is the first digital signature scheme recognized by any government

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)



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: encrypt(T) = (T^E) mod PQ
                                       = (T^17) mod 3233

The decryption function is: decrypt(C) = (C^D) mod PQ
                                       = (C^2753) mod 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
```

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 $s = \tilde{m}^d \bmod n$.
   (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 $\tilde{m} = s^e \bmod n$.
   (c) Verify that $\tilde{m} \in \mathcal{M}_R$; if not, reject the signature.
   (d) Recover $m = R^{-1}(\tilde{m})$.

Message Digest (One-way Bash) Functions

Message digest functions calculate a unique fixed-size bit string representation called Hash Value 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

Document

Message Digest Function

a14092af948b938569584e5b8d8d307a

Hash Value

Note: Message digests are also called one-way bash functions because they produce values that are difficult to invert

Message Digest Function: MD5


MD5 hash is a 32-digit hexadecimal number

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 is not collision resistant, use of latest algorithms such as SHA-1 and SHA-2 is recommended

It is widely used for digital signature applications, file integrity checking and storing passwords

Checksum Verifier

Calculate CRC & MD5

File	Size	CRC	MD5
batch_rename.png	14 472	18528C0A	EAF2C712F6E537AE1FEFD3FA1A4F4AAB
change_attributes.html	8 574	58101E09	E18D9F81CCF9A300F79321E8C768E021
change_attributes.png	7 957	2531FC3E	5E8A8FB259C7FDF790E5597C8154AF38
change_case.html	8 756	FC41186B	DDCAD7CF08BF7897D5B8B5F9806B47FD
change_case.png	6 821	2D34D339	04FED507091F5F095D977B358EC20EED
checksum_verify.png	8 117	3D8D9801	AC8AFE99B76BD1022AC7B2E34A7E1C49
convert.html	9 269	BE535A89	902BA23D7CC95EA2999CDA2EF1B27B41
convert.png	7 080	D760CFC6	F1176C7967E1DA2CA743D26DE9F1B0C0
convert_menu.png	8 735	638F8F0F	3F1BBD5E0B0B9E86970EDBA9705F14D4
file_comparator.html	8 575	44ED5DC4	959961C3E7D7559C9EE77965302A6E0A
file_comparator.png	17 787	D16F0E2B	C1AE1516BEABC17EDEFB58212D2C5331

clipboard hint | Save SFV... | Save MD5... | Close

Secure Hashing Algorithm (SHA)

NIST

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 $(2^{64} - 1)$ bits, 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

It is a future hash function standard still in development, chosen in a public review process from non-government designers

What is SSH (Secure Shell)?

Remote Communication

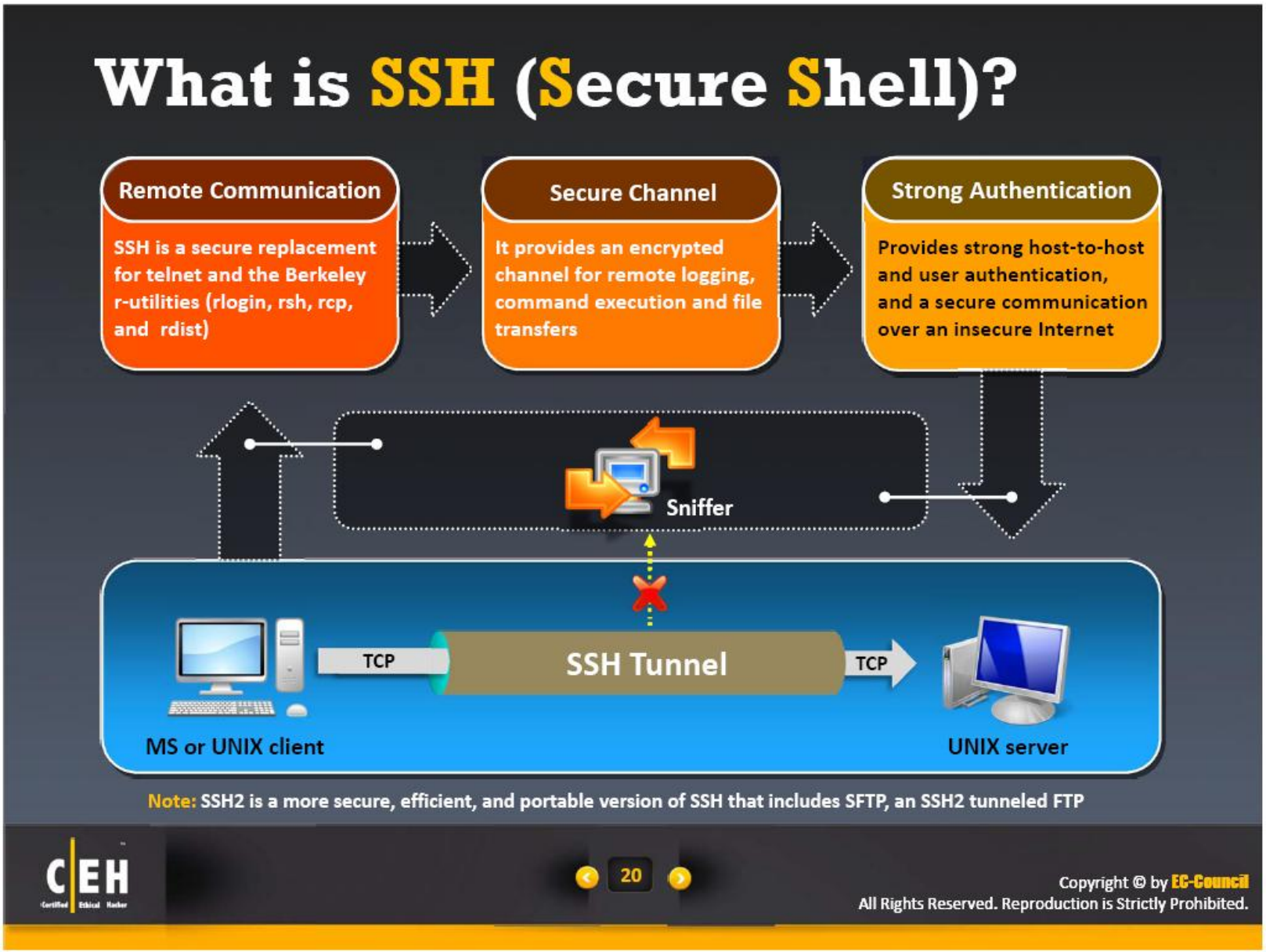
SSH is a secure replacement for telnet and the Berkeley r-utilities (rlogin, rsh, rcp, and rdist)

Secure Channel

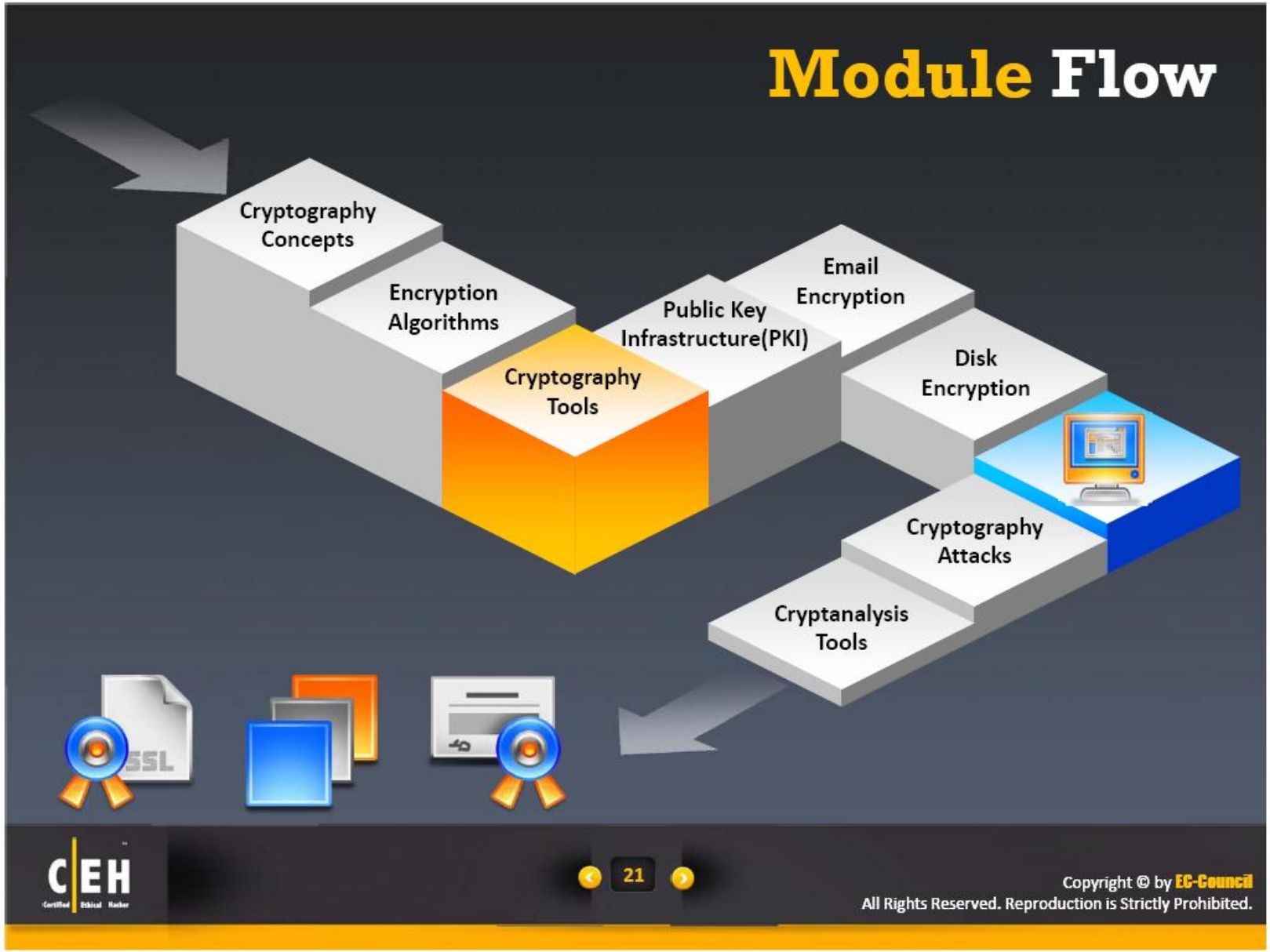
It provides an encrypted channel for remote logging, command execution and file transfers

Strong Authentication

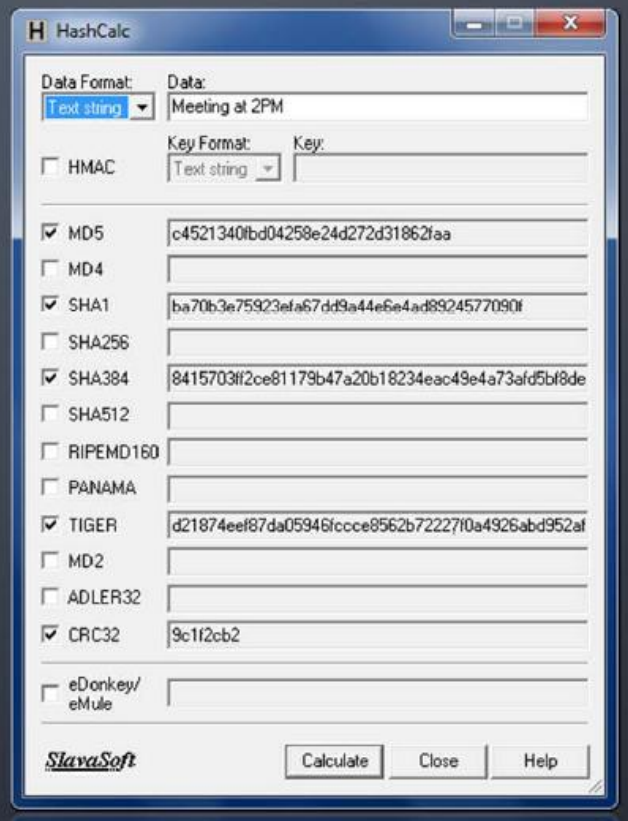
Provides strong host-to-host and user authentication, and a secure communication over an insecure Internet



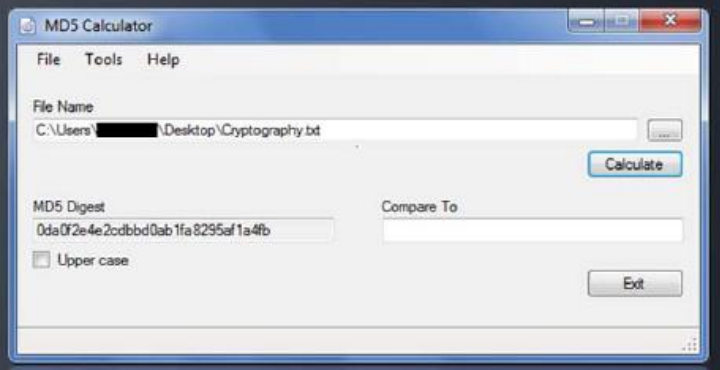
Note: SSH2 is a more secure, efficient, and portable version of SSH that includes SFTP, an SSH2 tunneled FTP



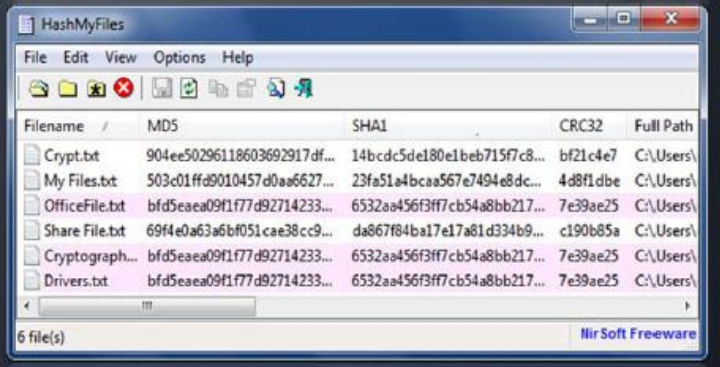
MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles



http://www.slavasoft.com

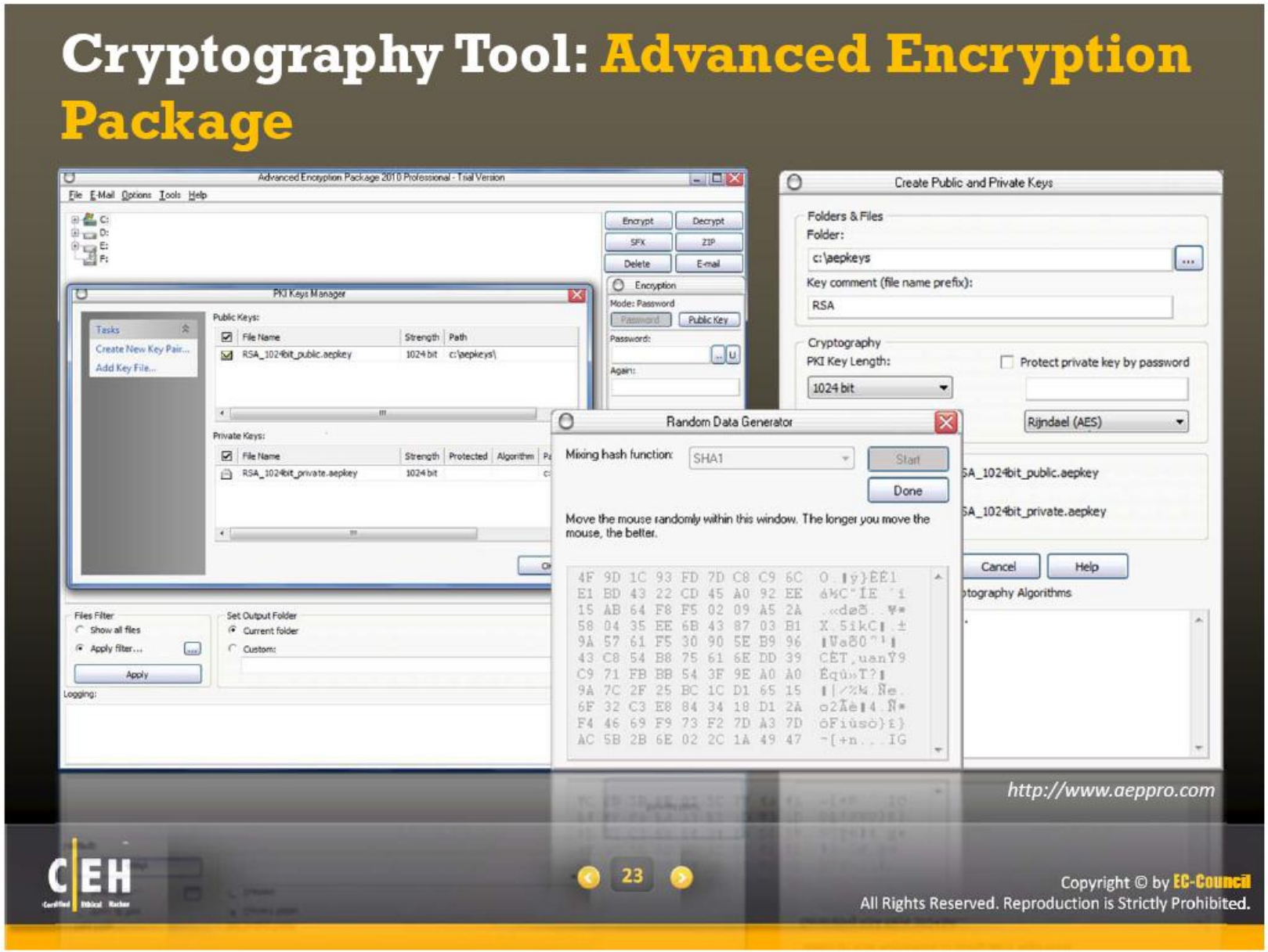


http://www.bullzip.com



http://www.nirsoft.net

Cryptography Tool: Advanced Encryption Package



Cryptography Tools

CommuniCrypt File Encryption Tool
http://www.communicrypt.com

CryptoForge
http://www.cryptoforge.com

Steganos LockNote
https://www.steganos.com

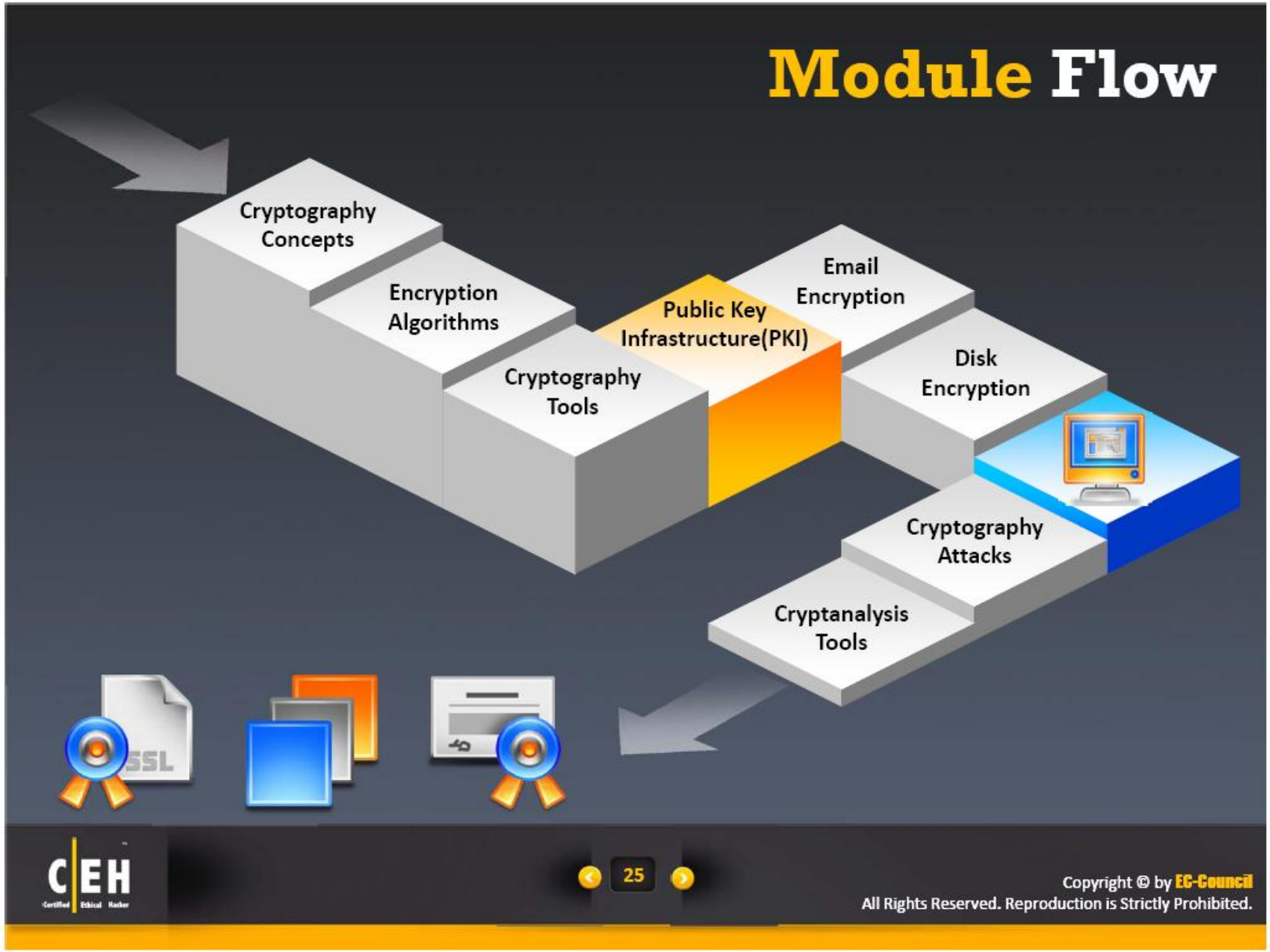
NCrypt XL
http://www.littlelite.net

AxCrypt
http://www.axantum.com

ccrypt
http://ccrypt.sourceforge.net

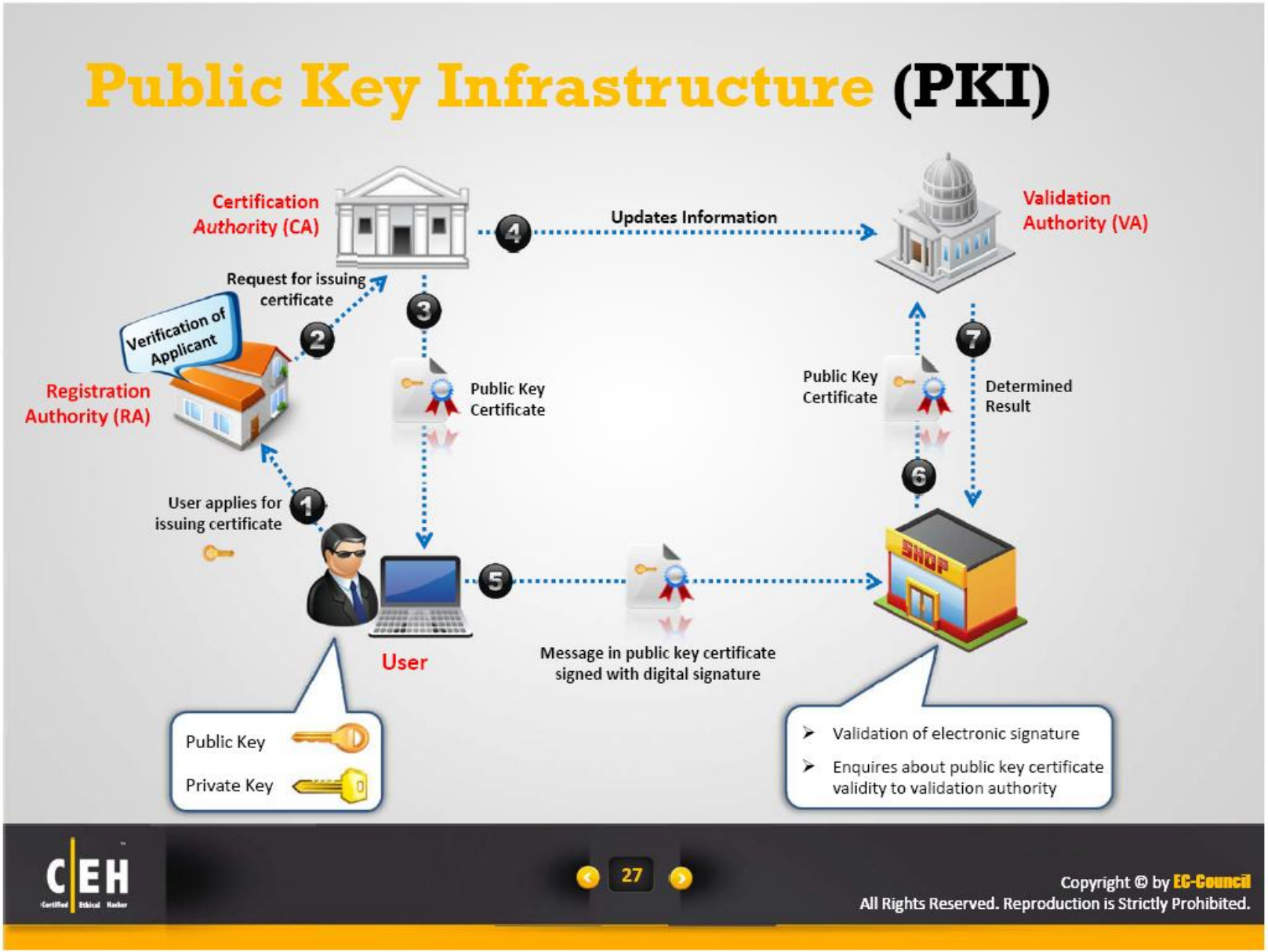
AutoKrypt
http://www.hiteksoftware.com

Cypherix
http://www.cypherix.com

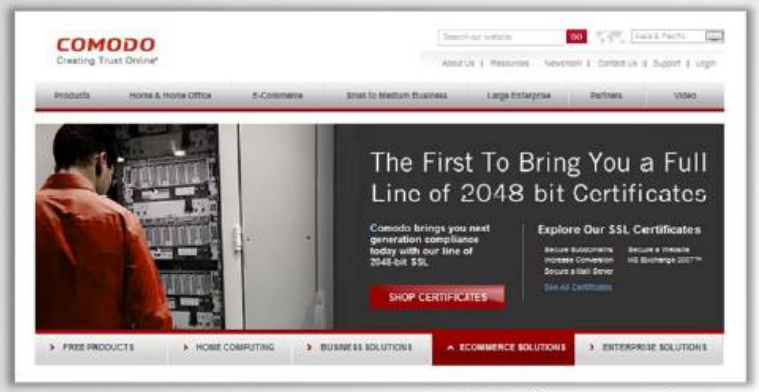


Public Key Infrastructure (PKI)

- 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



Certification Authorities

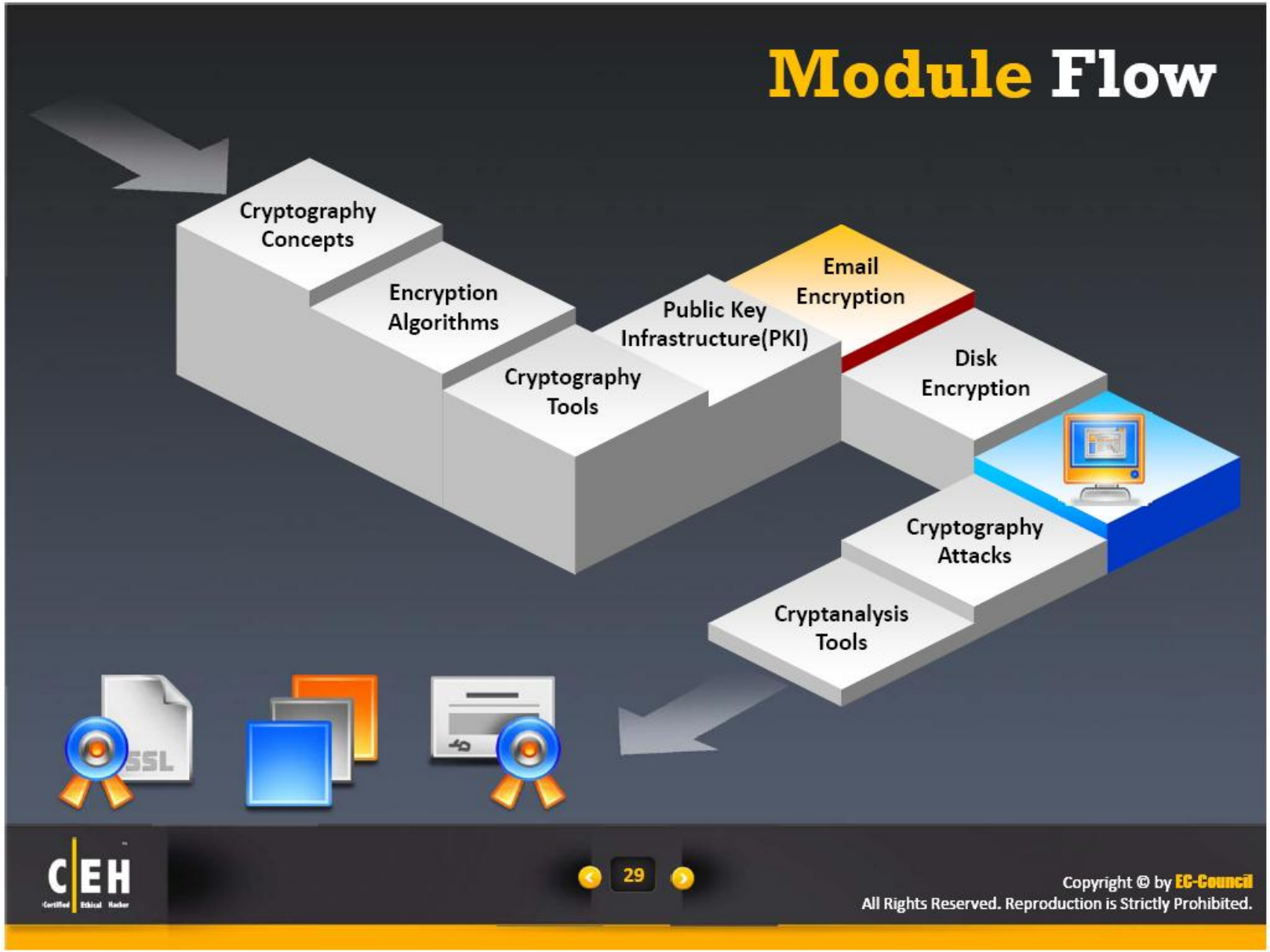


http://www.comodo.com

http://www.thawte.com

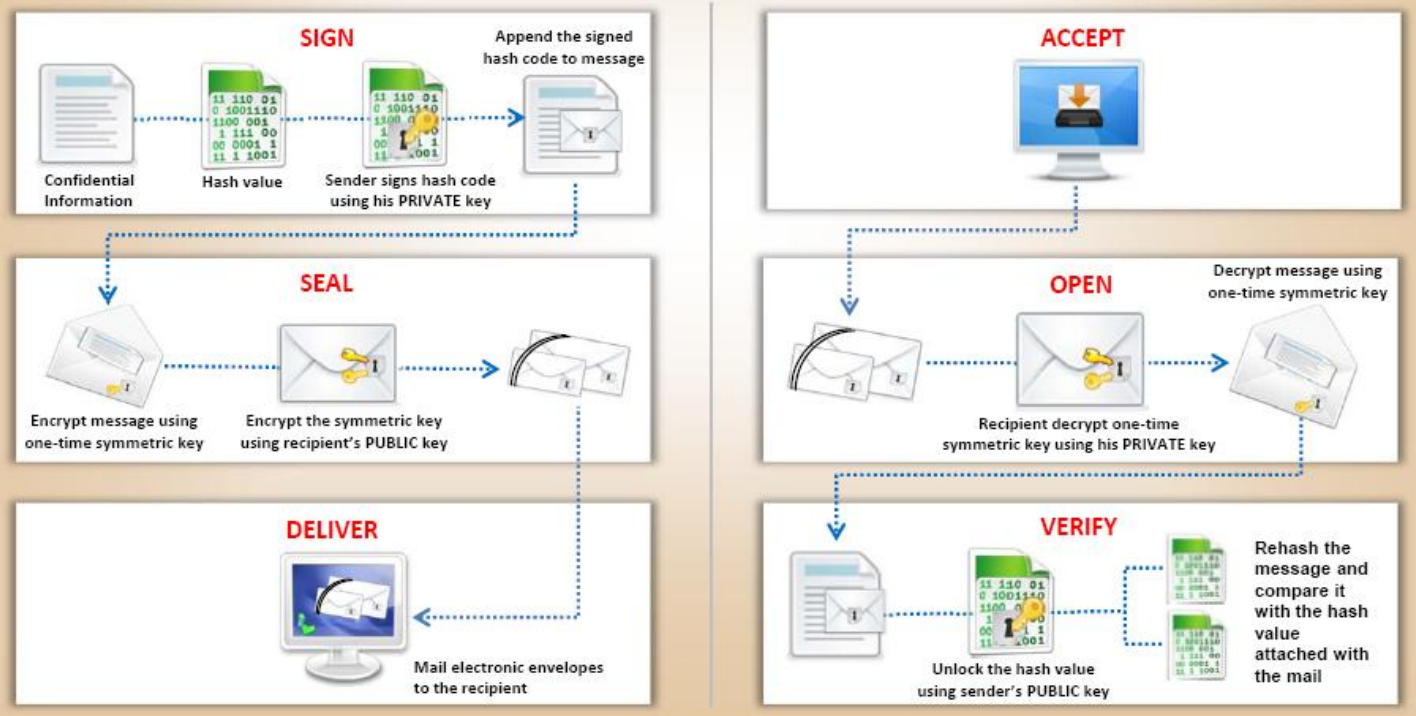
http://www.verisign.com

http://www.entrust.net



Digital Signature

- Digital signature used asymmetric cryptography to simulate the security properties of a **signature in digital, rather than written form**
- Digital signature schemes involve two algorithms; a **private key** for signing the message and a **public key** for verifying signatures



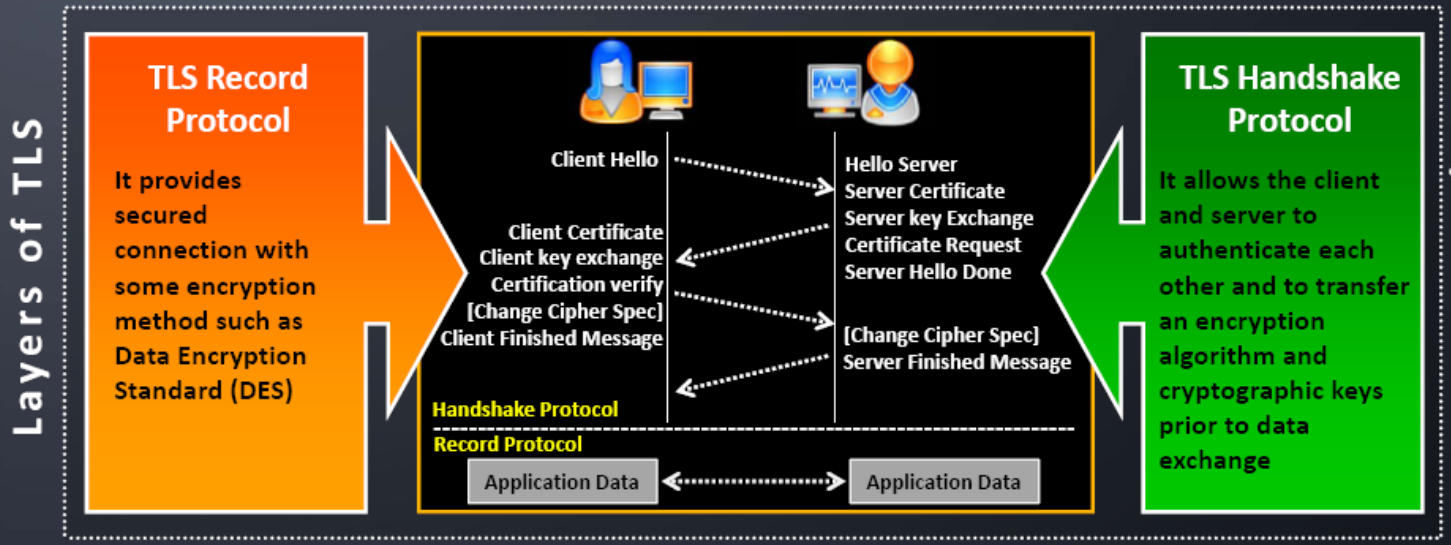
SSL (Secure Sockets Layer)

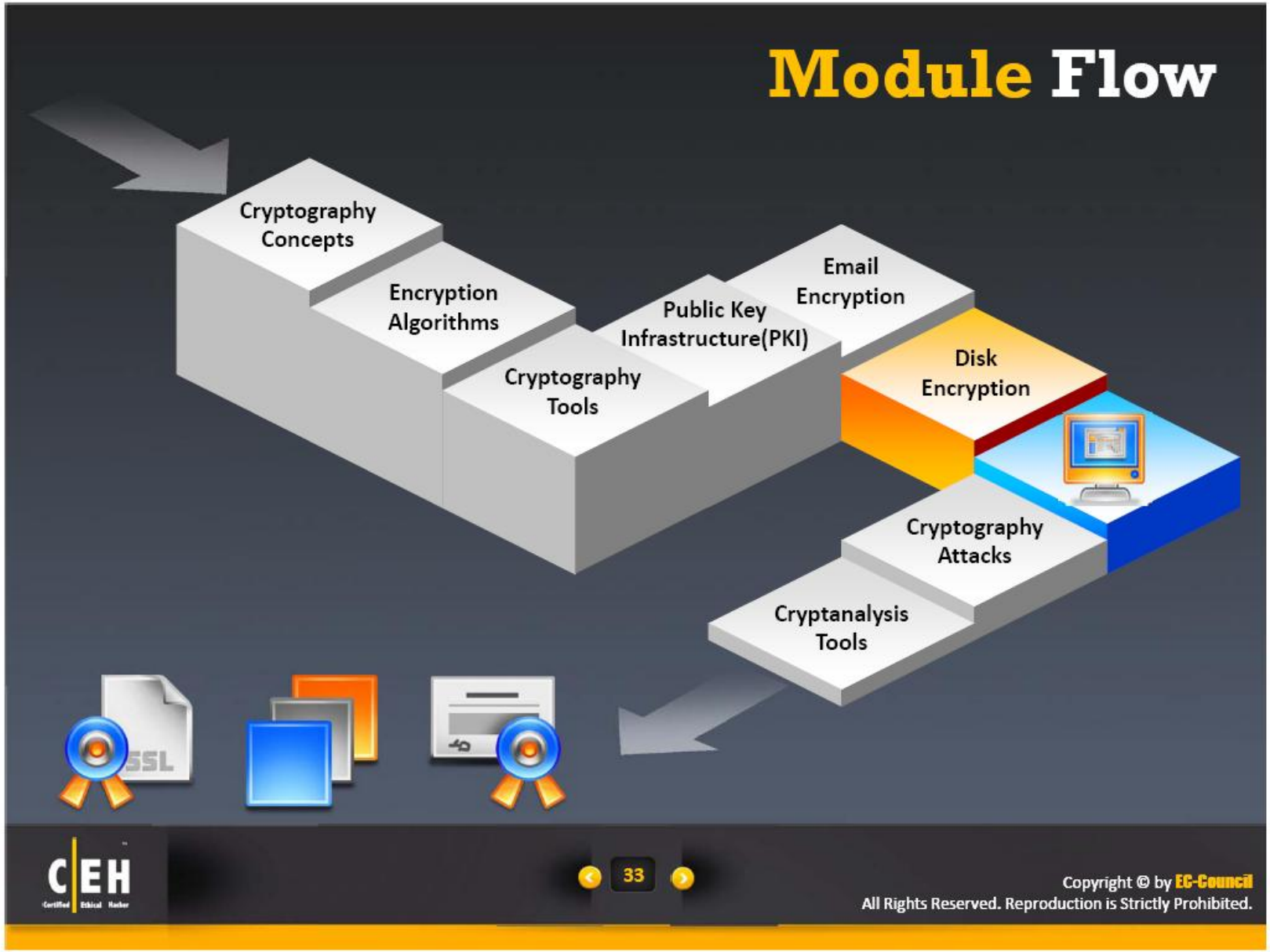
- SSL is an application layer protocol developed by Netscape for managing the security of a message transmission on the Internet
- It uses RSA asymmetric (public key) encryption to encrypt data transferred over a SSL connection

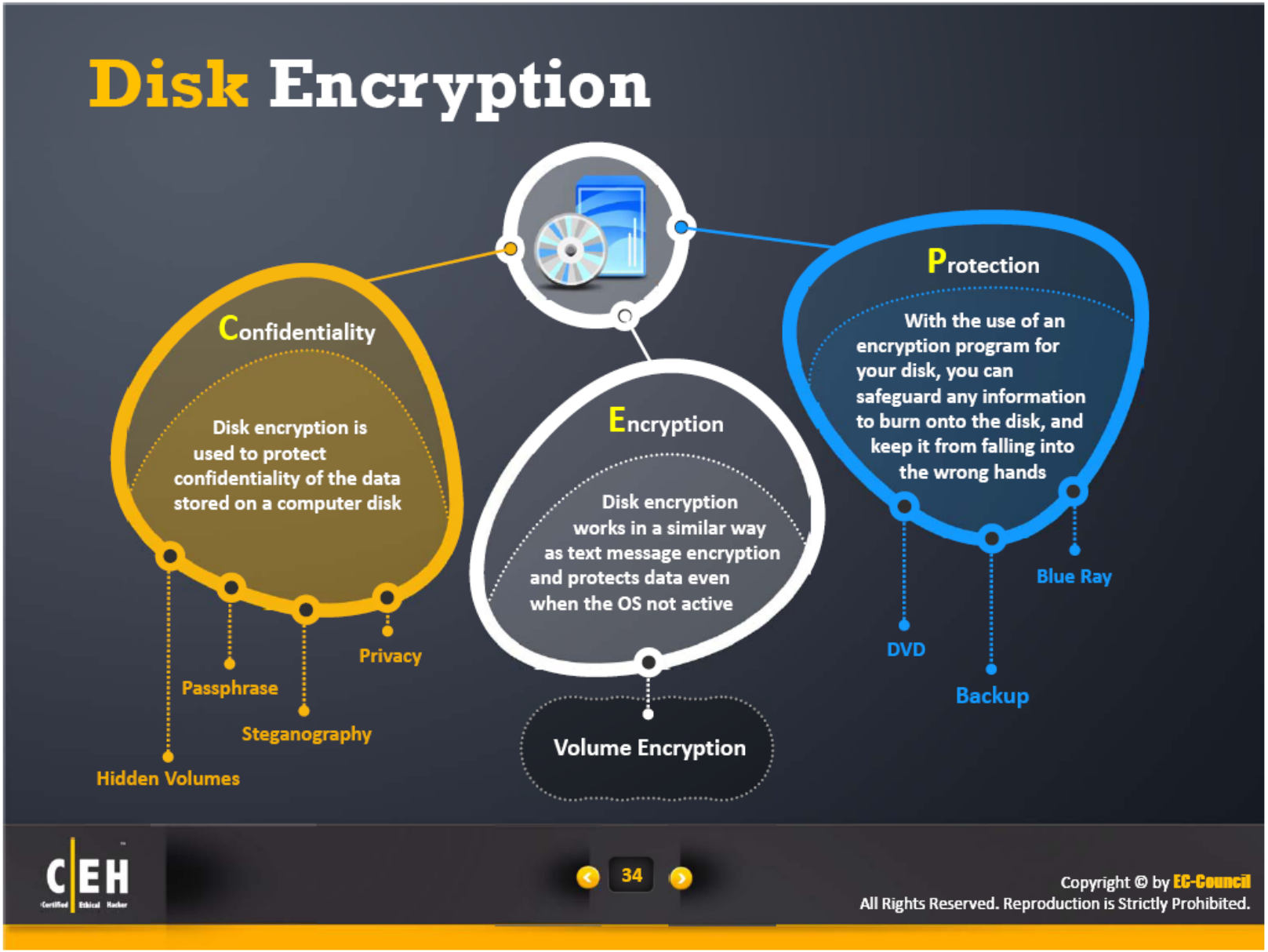
Transport Layer Security (TLS)

TLS is a protocol to establish a secure connection between a client and a server and ensure privacy and integrity of information during transmission

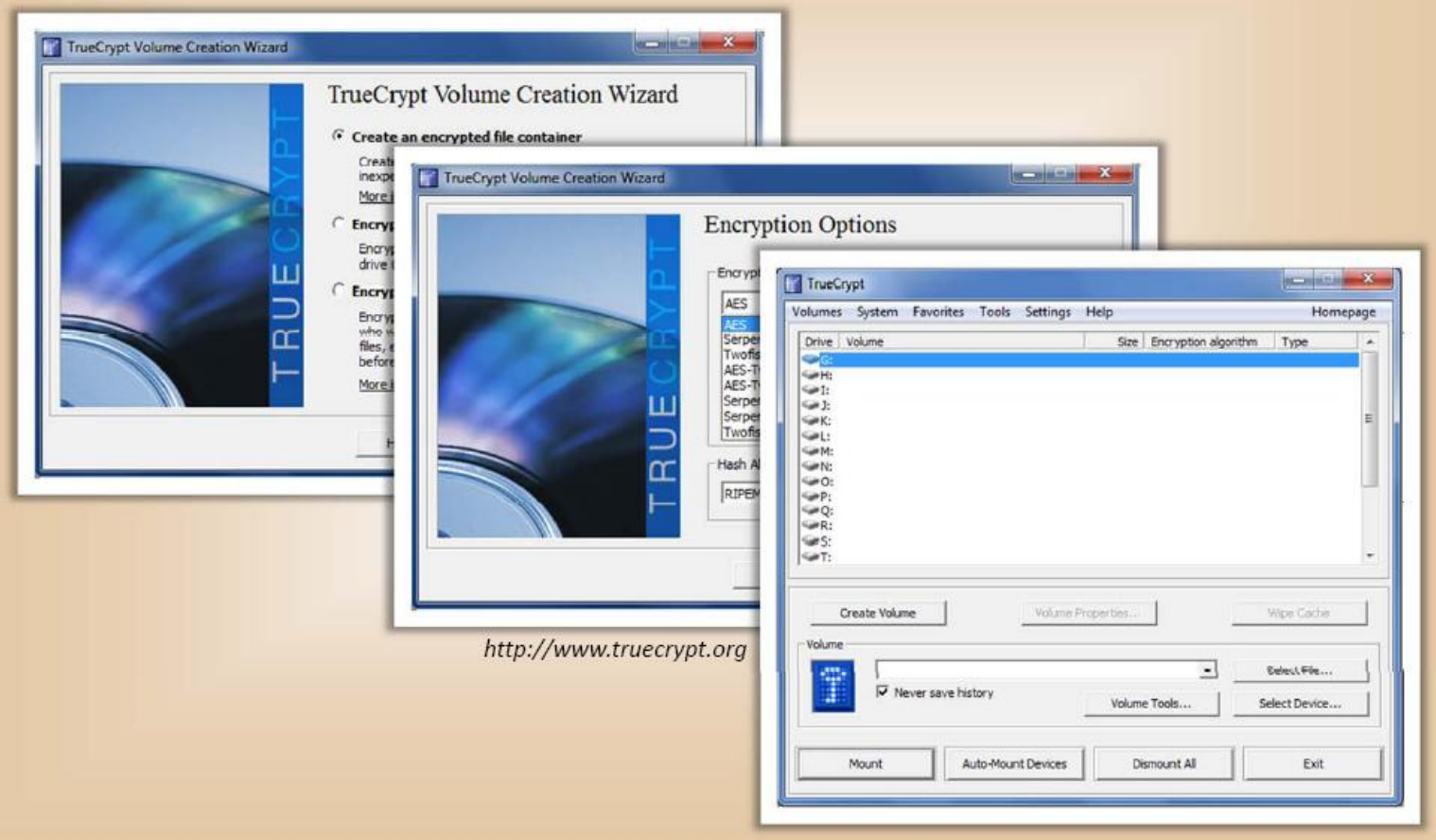
It uses RSA algorithm with 1024 and 2048 bit strengths






Disk Encryption
Confidentiality
Disk encryption is used to protect confidentiality of the data stored on a computer disk
Privacy
Passphrase
Steganography
Hidden Volumes
Encryption
Disk encryption works in a similar way as text message encryption and protects data even when the OS not active
Volume Encryption
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
DVD
Backup
Blue Ray
C|EH
34
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Disk Encryption Tool: TrueCrypt



http://www.truecrypt.org

Disk Encryption Tools

DriveCrypt
http://www.securstar.com

BitLocker
http://www.microsoft.com

ShareCrypt
http://www.securstar.comm

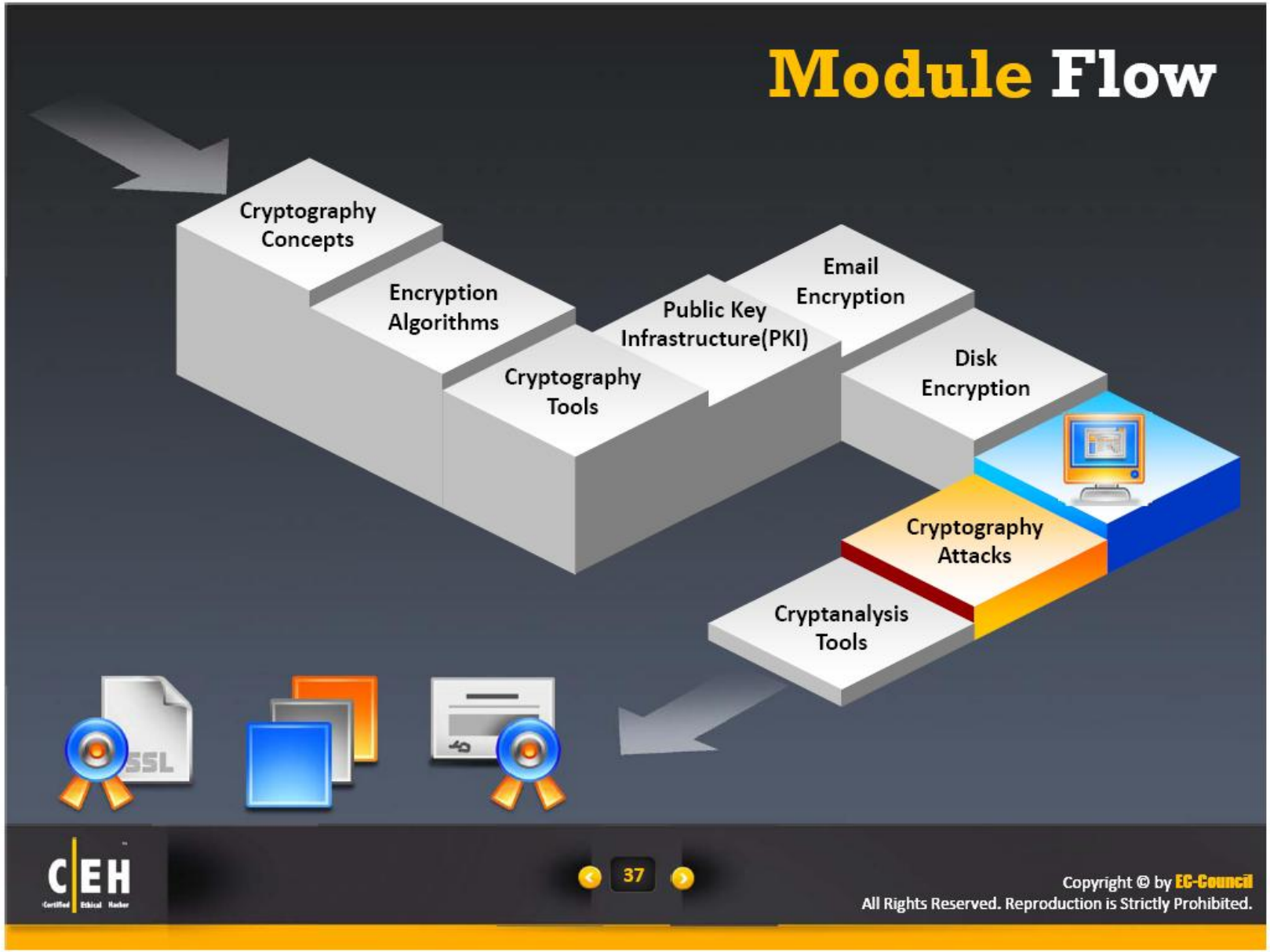
DriveCrypt Plus Pack
http://www.securstar.com

PocketCrypt
http://www.securstar.com

Master Voyager
http://www.mvoyager.com

FreeOTFE / FreeOTFE4PDA
http://www.freeotfe.org

FreeOTFE Explorer
http://www.freeotfe.org



Cryptography Attacks

Cryptography attacks are based on the assumption that the cryptanalyst has knowledge of the encrypted information

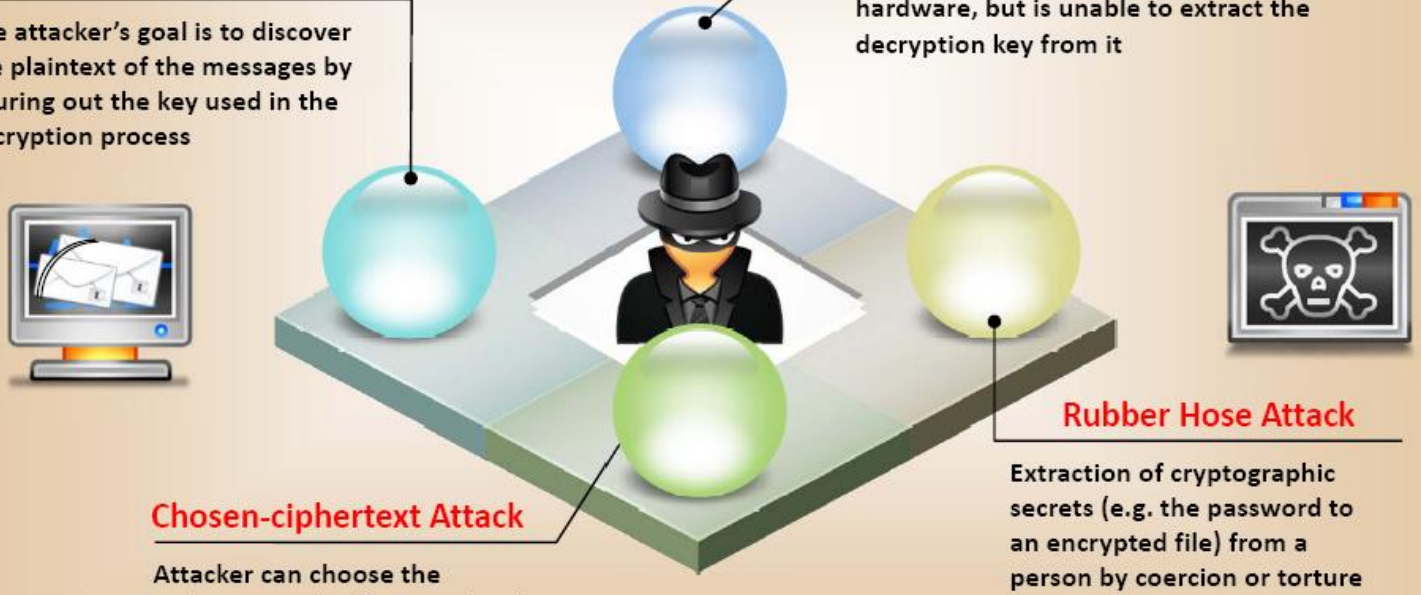
Cryptography Attacks

Adaptive Chosen-plaintext Attack

Attacker uses this technique when he has free use of a piece of decryption hardware, but is unable to extract the decryption key from it

Ciphertext-only Attack

The attacker's goal is to discover the plaintext of the messages by figuring out the key used in the encryption process



Rubber Hose Attack

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

Chosen-ciphertext Attack

Attacker can choose the ciphertext to be decrypted and has access to the resulting decrypted plaintext

Cryptography Attacks

Chosen-plaintext

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

Known-plaintext Attack

- The attacker's goal is to discover the key used to encrypt the messages so that other messages can be deciphered and read

Chosen-key Attack

- A generalization of the chosen-text attack

Timing Attack

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

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

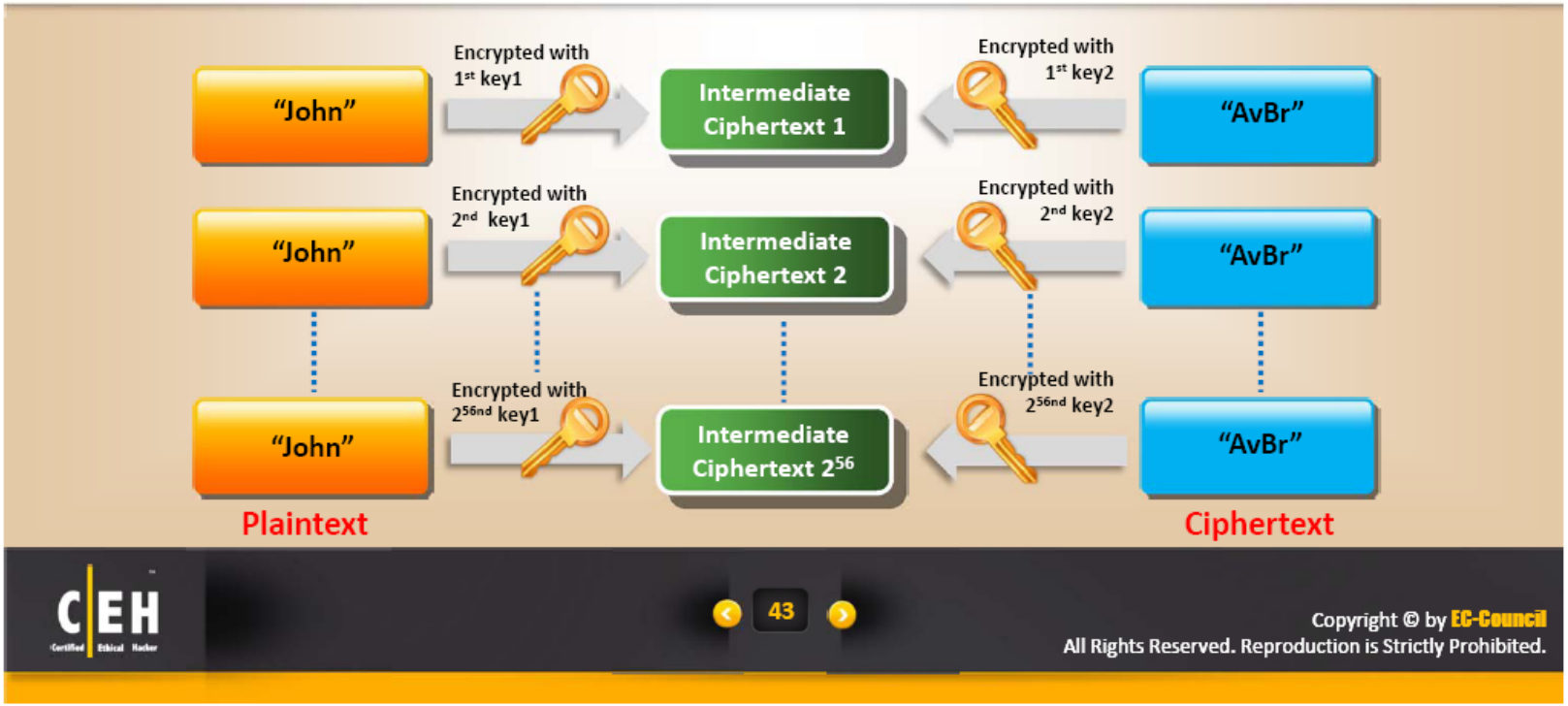
Brute-Force Attack

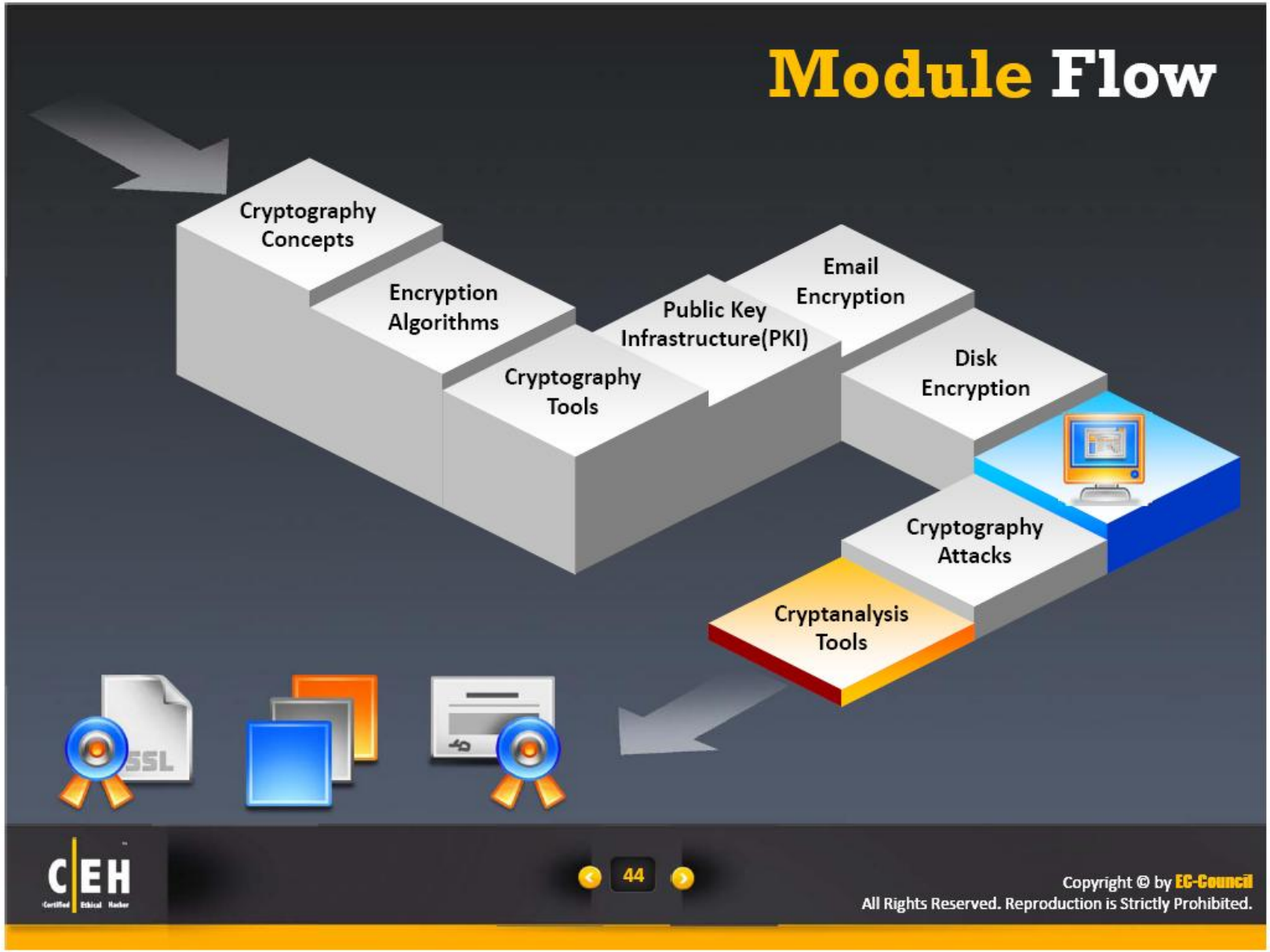
Power/Cost	40 bits (5 char)	56 bit (7 char)	64 bit (8 char)	128 bit (16 char)
$ 2K (1 PC. Can be achieved by an individual)	1.4 min	73 days	50 years	10^20 years
$ 100K (this can be achieved by a company)	2 sec	35 hours	1 year	10^19 years
$ 1M (Achieved by a huge organization or a state)	0.2 sec	3.5 hours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

Estimate Time for Successful Brute – Force Attack

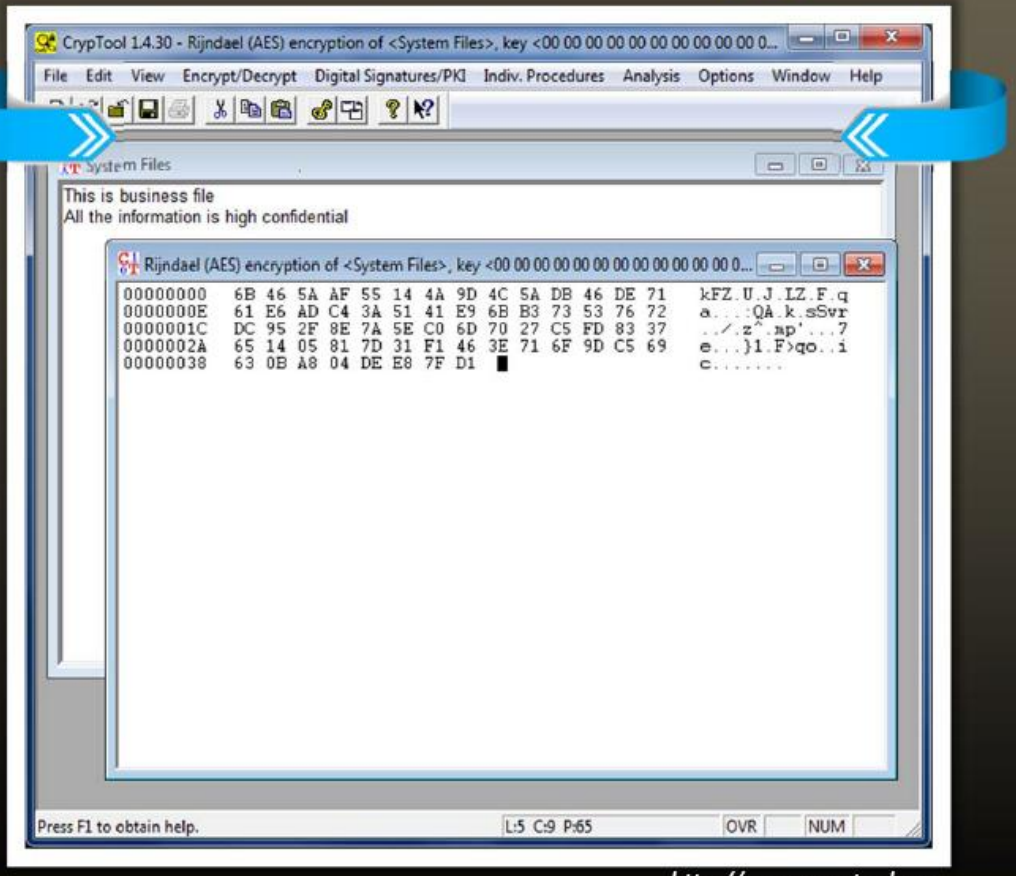
Meet-in-the-Middle Attack on Digital Signature Schemes

- The meet-in-the-middle attack **breaks a cipher** into two parts, works against each separately, and compares results
- It can be used for **forging signatures** on mixed-type digital signature schemes, and takes less time than an exhaustive attack
- The attack works by **encrypting from one** end and **decrypting from the other end**, thus meeting in the middle




Module Flow
Cryptography Concepts
Encryption Algorithms
Cryptography Tools
Public Key Infrastructure(PKI)
Email Encryption
Disk Encryption
Cryptography Attacks
Cryptanalysis Tools
SSL
CEH
44
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Cryptanalysis Tool: CrypTool



http://www.cryptool.org

Cryptanalysis Tools

Cryptanalysis
http://studenthome.nku.edu

Ganzúa
http://ganzua.sourceforge.net

Cryptanalysis Tools
http://cryptanalysisto.sourceforge.net

Crank
http://crank.sourceforge.net

CryptoBench
http://www.addario.org

EverCrack
http://evercrack.sourceforge.net

JCrypTool
http://jcryptool.sourceforge.net

AlphaPeeler
http://sourceforge.net

Online MD5 Decryption Tool

md5
http://md5.rednoize.com

md5crack
http://md5crack.com

MD5 Decrypter
http://www.md5decrypter.com

Hash Cracking Tool
http://www.tmto.org

MD5Cracker
http://md5cracker.tk

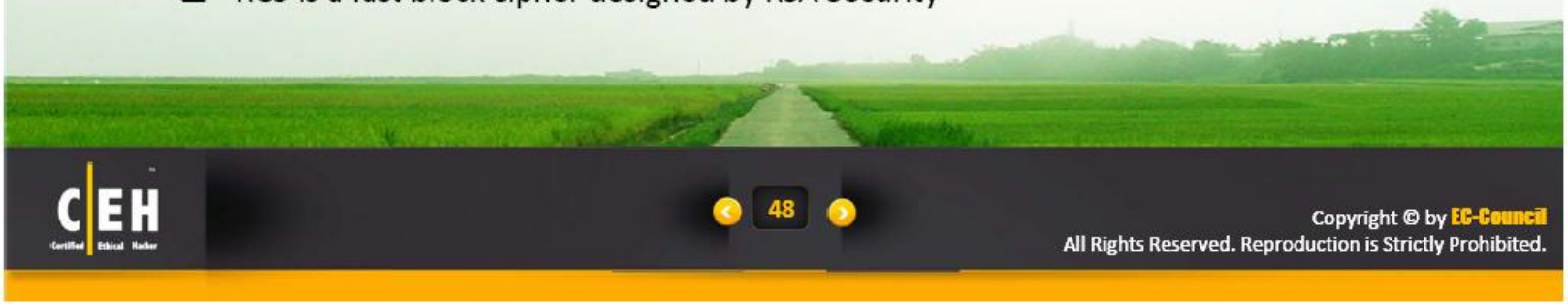
Hash Cracker
http://www.hash-cracker.com

Passcracking
http://passcracking.com

MD5Decrypter
http://www.md5decrypter.co.uk

Module Summary

- Using Public Key Infrastructure (PKI), anyone can send a confidential message using public information, which can only be decrypted with a private-key in the sole possession of the intended recipient
- RSA encryption is widely used and is a de-facto encryption standard
- The MD5 algorithm is intended for digital signature applications, where a large file must be compressed securely before being encrypted
- SHA algorithm takes a message of arbitrary length as input and outputs a 160-bit message digest of the input
- Secure Sockets Layer, SSL is a protocol for transmitting private documents via the Internet
- RC5 is a fast block cipher designed by RSA Security



Quotes

"Programming can be fun, so can cryptography; however they should not be combined."

- Kreitzberg and Shneiderman, Authors