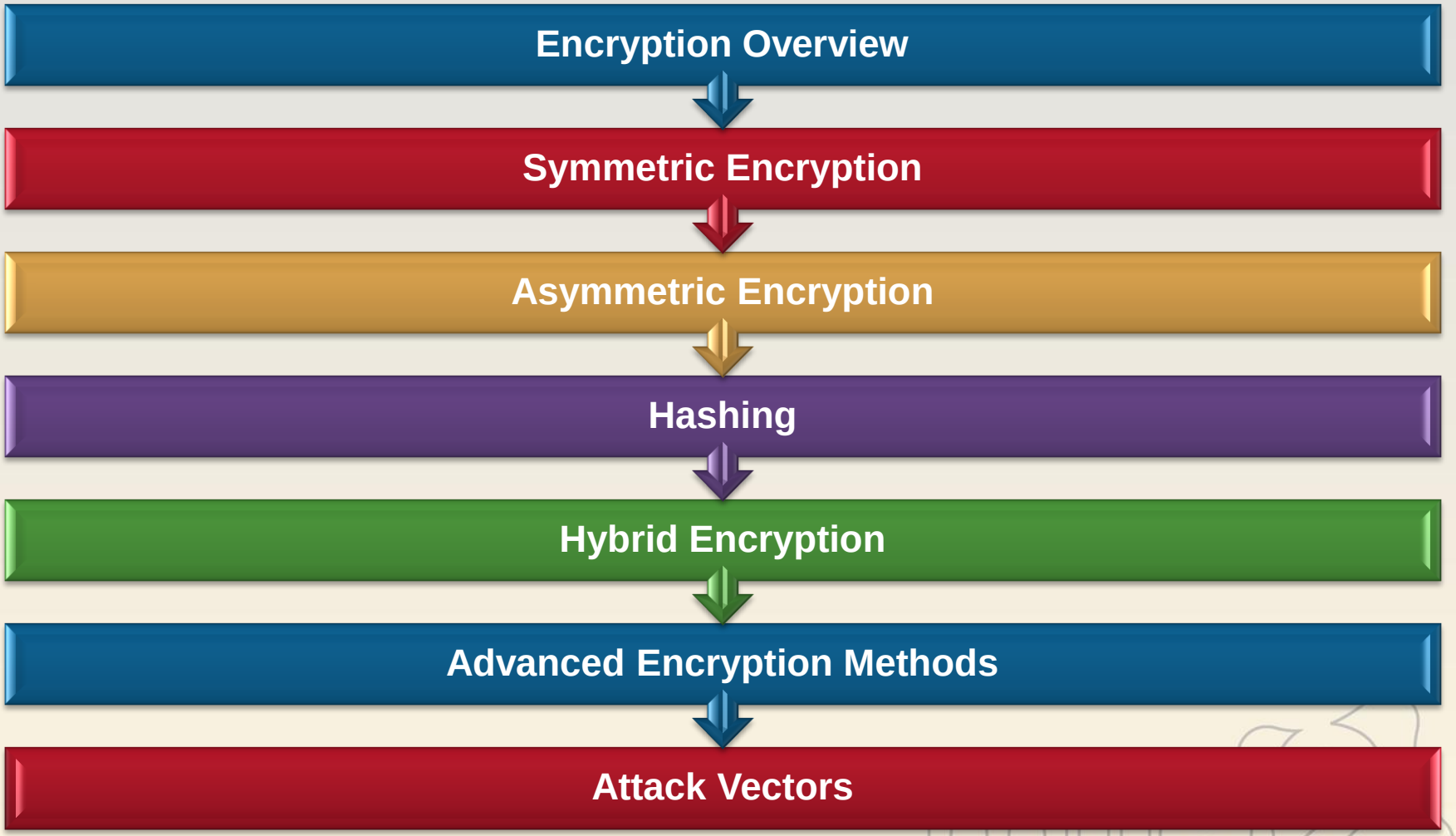
Cryptography Decrypted

Overview



Introduction

Encryption has been used throughout history. The Egyptians used Hieroglyphics, Caesar used Substitution Cipher, Spartans used Skytale, and Thomas Jefferson used a Cipher wheel.

Skytale was a thin sheet of papyrus wrapped around a stick

As systems have become more complex and the data to protect more valuable, cryptography methods have also evolved.

IPSec, PKI, Quantum Cryptography, PGP, Elliptic Curves, etc.

There are many different algorithms and applications that are used to keep information safe in today's corporate networked environment.

Encryption

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge- a key

Encryption also implicitly refers to the reverse process, decryption, to make the encrypted information readable again (i.e. to make it unencrypted)..

Encryption, by itself, can protect the confidentiality of messages but other techniques are still needed to protect the integrity and authenticity of a message

Message Authentication Code (MAC) and Digital Signatures are examples of Integrity and Non-Repudiation mechanisms.

http://en.wikipedia.org/wiki/Encryption

Cryptographic Definitions

Cryptography

- Science of hiding the meaning of communication

Cipher

- Something that transforms characters or bits into an unreadable format
  - Usually used as another name for an algorithm

Cryptographic Algorithm

- Procedures that turn readable data into an unreadable format
  - Today this takes place through complex mathematical formulas

Cryptanalysis

- Science of studying and breaking encryption mechanisms
  - White and black hat

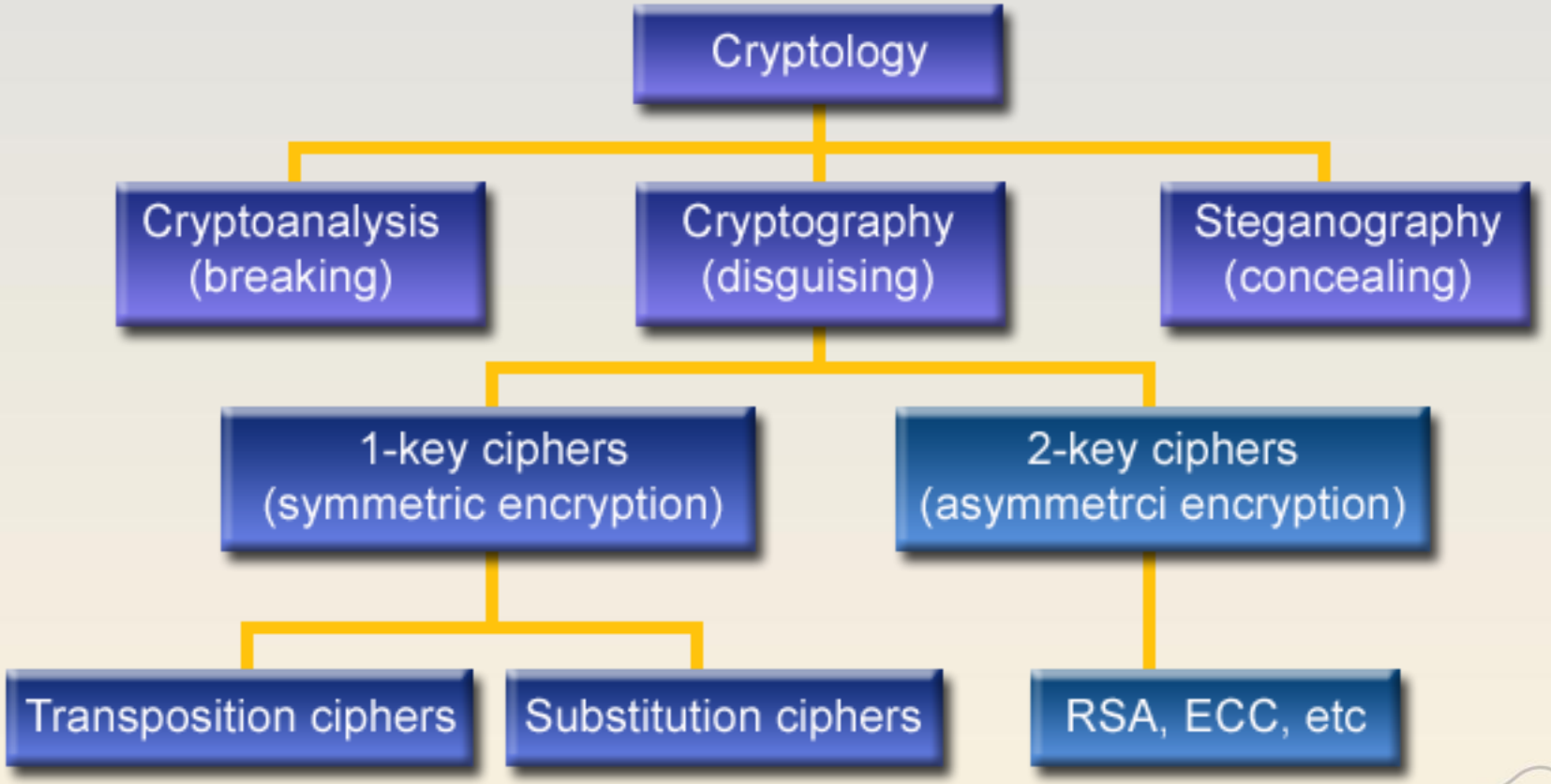
Cryptology

- Study of cryptography and cryptanalysis
  - Cryptographers work in the field of cryptology

Key Clustering

- When two keys generate the same ciphertext from the same plaintext

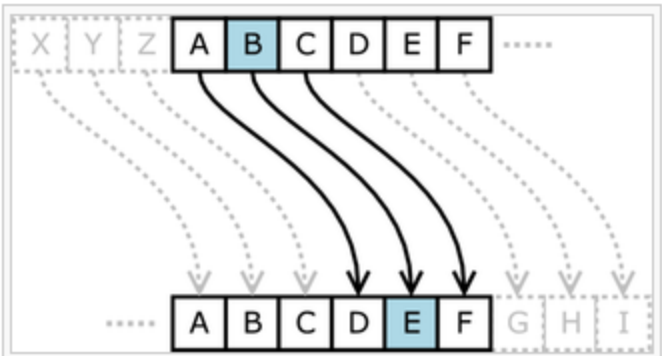
The Science of Secret Communication



Encryption Algorithm

A mathematical procedure for performing encryption on data. Through the use of an algorithm, information is made into meaningless cipher text and requires the use of a key to transform the data back into its original form.

Example:



The action of a Caesar cipher is to move each letter a number of places down the alphabet. This example is with a shift of three, so that a B in the plaintext becomes E in the ciphertext.

http://www.webopedia.com/TERM/e/encryption_algorithm.htm

Implementation

There are two main methods of implementing encryption, Block and Stream ciphers.

Block cipher is a type of symmetric key cipher which operates on blocks or groups of bits of a fixed or unvarying length.

The National Institute of Standards and Technology (NIST) is a federal agency that approved the Data Encryption Standard (DES) block cipher.

Another standard developed in the 1980s is the Triple Data Encryption Standard (3DES).

Some commonly used block cipher algorithms are IDEA, RC2, RC5, CAST and Skipjack.

Stream cipher is a symmetric cipher in which the input digits are encrypted successively or one at a time, and in which the transformation of successive digits varies during the encryption.

Stream ciphers typically execute at a higher speed than block ciphers and have lower hardware complexity.

Symmetric Encryption

Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related cryptographic keys for both decryption and encryption.

The encryption key is trivially related to the decryption key, in that they may be identical.

The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.

Speed:

Symmetric-key algorithms are generally much less computationally intensive than asymmetric key algorithms.

http://en.wikipedia.org/wiki/Symmetric_key

Symmetric Encryption

Limitations:

The disadvantage of symmetric-key algorithms is the requirement of a *shared secret key*, with one copy at each end. Since keys are subject to potential discovery by a cryptographic adversary, they need to be changed often and kept secure during distribution and in service.

Example= WEP
(Wired Equivalent Privacy)

A three-rotor German military Enigma machine showing, from bottom to top, the plugboard, the keyboard, the lamps and the finger-wheels of the rotors emerging from the inner lid (version with labels).

http://en.wikipedia.org/wiki/Enigma_machine

Symmetric Downfalls

Weaknesses

- Key distribution **– It requires a secure method to get the key to the destination**
- Scalability – **Each pair of users need a unique pair of keys, so the number of keys can grow and become unmanageable**
- Limited security – **It can provide confidentiality, but not true authenticity or non-repudiation**

Symmetric Algorithms

Name	Block Size	Key Size (in bits)
Advanced Encryption Standard (Uses Rijndael algorithm)	Variable	128, 192, 256
Triple Data Encryption Standard (3DES)	64	168
Data Encryption Standard (DES)	64	56
International Data Encryption Algorithm (IDEA)	64	128
Blowfish	Variable	1-448
Twofish	128	1-256
Rivest Cipher 5 (RC5)	32,64,1280 -2048	
Carlisle Adams/Stafford Tavares (CAST-128)	64	128

Crack Times

DES (the Data Encryption Standard) is not considered valid for information that we want to keep classified.

DES has an effective key length of 56 bits, which gives a “key space” of >72 quadrillion possible keys.

DES was replaced by the AES (the Advanced Encryption Standard) with effective key lengths of 128, 192, and 256 bits.

That makes possible key space (at 256 bits) of 1.15792089237316195423570985008 69e+77

To put it into perspective; if a machine exists that can crack DES in one second, it would take that same machine 149 trillion years to crack AES at 128 bits!

Asymmetric Encryption

Asymmetric encryption utilizes two separate keys (Private & Public), one to encrypt, the other to decrypt.

These keys are generated at the same time and are related to each other.

The private key is kept secret, while the public key may be widely distributed – email or online servers.

The first invention of asymmetric key algorithms came in the early 1970s; later becoming known as the Diffie-Hellman key exchange.

RSA Security was founded by the authors of the RSA Algorithm which is based on the factoring of large prime numbers.

RSA is an acronym of the authors: Ronald L Rivest, Leonard Adleman and Adi Shamir who were all professors at MIT when they published their paper in 1977.

Public Key Cryptography Advantages

Asymmetric Addresses Problems Uncovered in Symmetric Algorithms

- Easily scaled
  - Asymmetric only requires each user to have one pair of keys
  - 1,000 users = 2,000 keys
- Does not require "out-of-band" delivery of key
  - Public key is distributed and needs no protection
- Provides true authenticity and non-repudiation

Asymmetric Algorithm Disadvantages

Very Slow Compared to Symmetric Cryptography

- Up to 1,000 times slower
  - Uses more complex mathematical formulas

Size of Encrypted Data Limited by Key Length

- Can only be used to encrypt smaller amounts of data

Asymmetric Algorithm Examples

Asymmetric Algorithms

- RSA
- Elliptic Curve Cryptosystem (ECC)
- Diffie-Hellman
- El Gamal
- Knapsack

Key Exchange

Diffie-Hellman key exchange (D-H) is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel

This key can then be used to encrypt subsequent communications using a symmetric key cipher.

ElGamal is an asymmetric system that is based on DH.

Asymmetric encryption is not very efficient.

Symmetric versus Asymmetric

Attributes	Symmetric	Asymmetric
Keys	One Key is Shared Between Two or More Entities	Each Entity has a Public/Private Key Pair
Key Exchange	Out-of-Band	Public Key is Safely Distributed
Speed	Algorithm is Less Complex and Faster	Algorithm is More Complex and Slower
Number of Keys	Grows as Number of Users Grow	Does not grow uncontrollably
Use	Bulk Encryption, which means Encrypting Files and Communication Paths	Key Encryption and Distribution
Security Service Provided	Confidentiality	Confidentiality, Authentication and Non-Repudiation

Using the Algorithm Types Together

Sender Steps

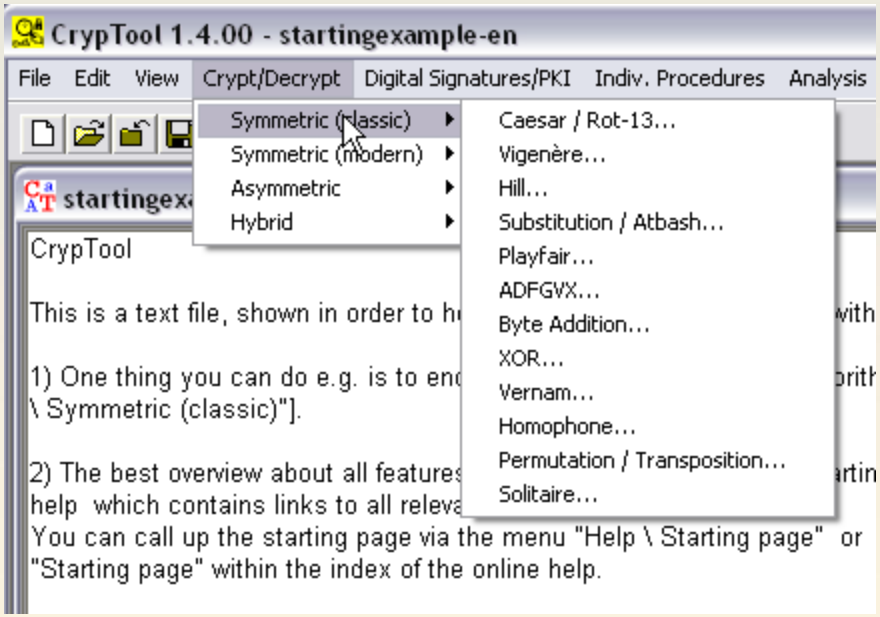
- Symmetric key is used to encrypt message
- Asymmetric key (receiver's public key) is used to encrypt symmetric key
- Both are sent to destination

Receiver Steps

- Uses symmetric key to decrypt message
- Decrypts symmetric key with receiver's private key

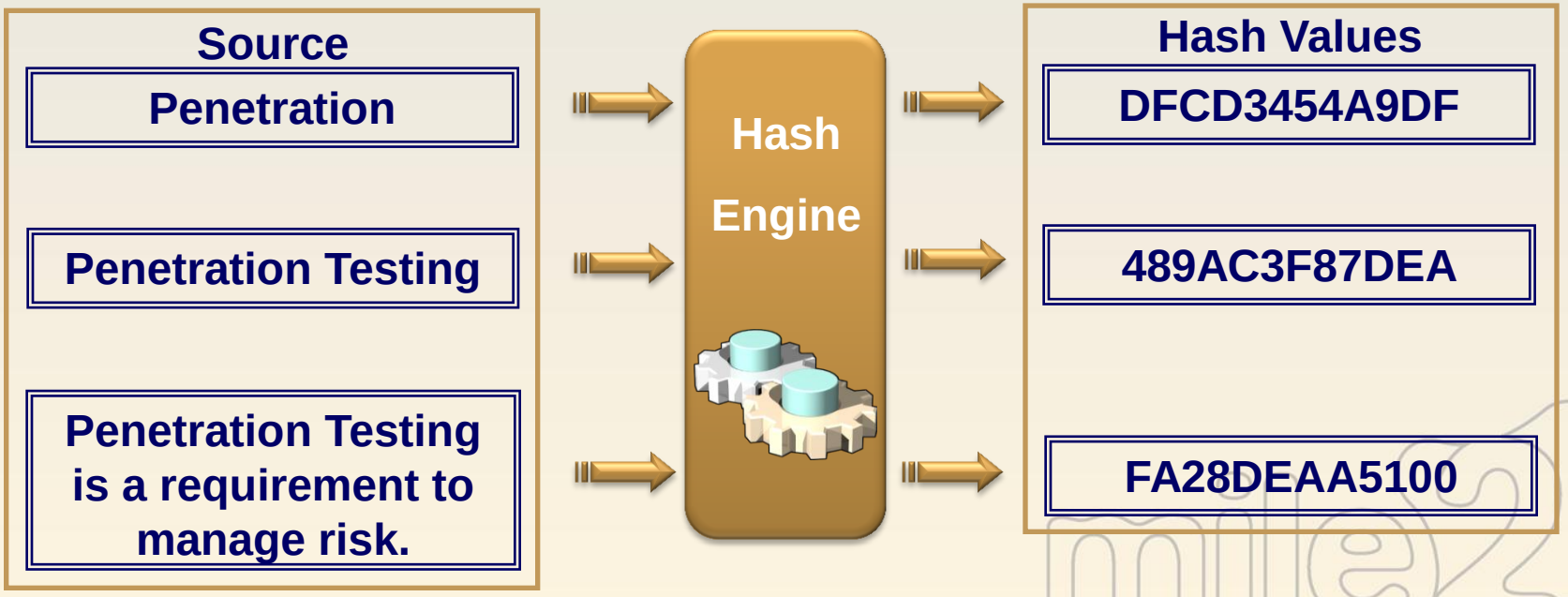
Instructor Demonstration

Instructor will demonstrate using CrypTool to help you understand various encryption methods.



Hashing

- A hash is a process to create a unique string of characters from any data source– password, executable etc.
- The output is of a fixed length defined by the algorithm.
- The output changes completely if the source changes.
- It is used mainly for data integrity and secure password authentication.
- The hash cannot be reversed to the plain text – one way.



Common Hash Algorithms

Message Digest Family

MD4 (cracked!)

- 128 bits – used to hash local Windows passwords.

MD5 (cracked!)

- 128 bits – used in many systems for data integrity.

Secure Hashing Algorithm

SHA1 (cracked – maybe!)

- 160 bits – used as industry standard & XBOX copy protection!

SHA2

- 224,256,384 & 512 bits – should be used above all others.

Have a look at the different outputs online:

http://serversniff.net/hash.php

Birthday Attack

Mathematical Paradox

- How many people have to be in the same room for there to be over a 50% chance that someone has the same birthday as you?
  - 253 people
- How many people have to be in the same room for there to be over a 50% chance that two people have the same birth date?
  - 23 people

Hashing Issue

- It is easier to find two messages that have the same MD value than looking for one particular MD value on a message
- Hashing value = n Brute force to find one specific hash value = 2^n Brute force to find any two matching hash values = $2^{(n/2)}$
- Crux = A hashing algorithm that generates a larger MD value is less vulnerable to a birthday attack than an algorithm that creates a smaller MD value

Example of a Birthday Attack

Bob and Sue create a document before they get married indicating that they will split everything 50/50 if they get a divorce.

They put this through a hashing algorithm and generate MD value X.

Later, Sue makes many copies of the document and slightly changes each one to indicate that she gets everything after a divorce.

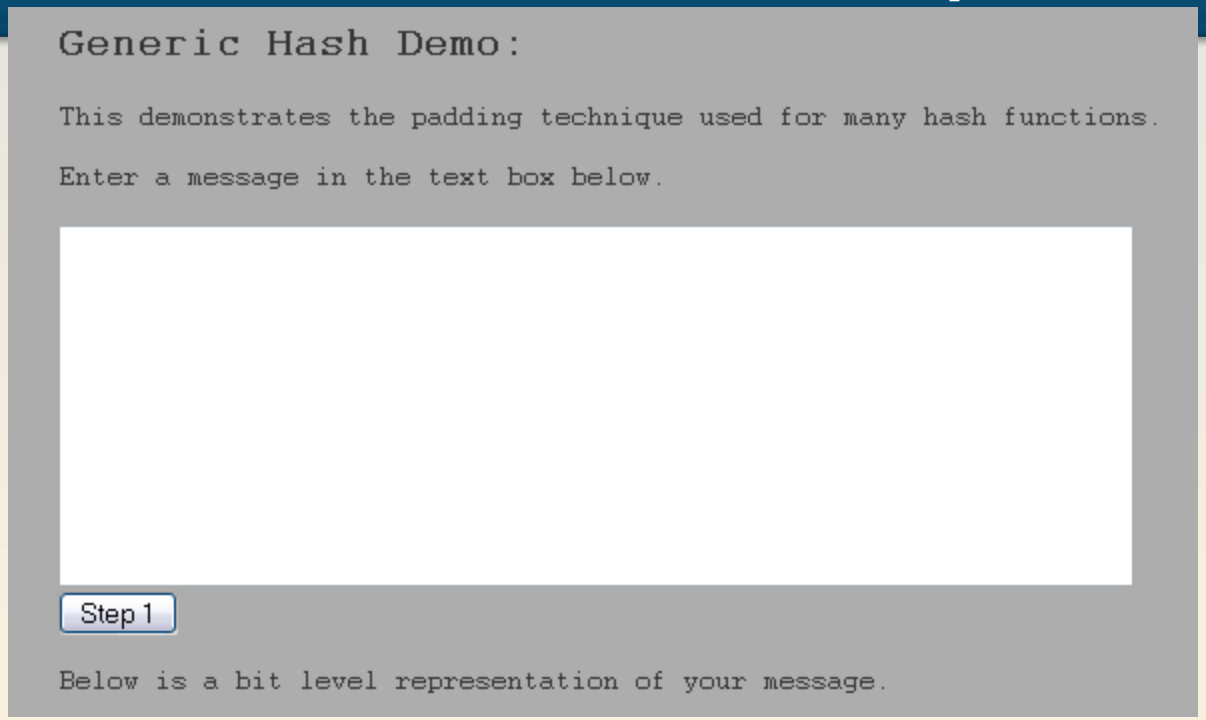
Sue runs them all through the same hashing algorithm until one has the same MD value as the original.

A collision takes place

Sue swaps the original document with her new document.

Generic Hash Demo

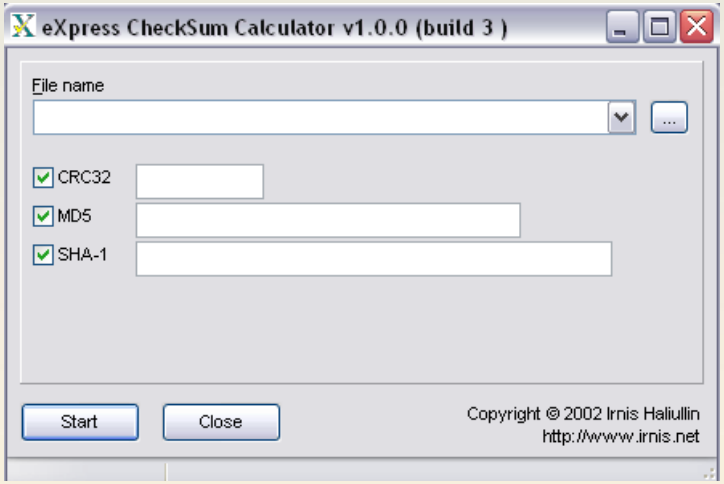
Instructor will demonstrate the process to create a hash from a text input:

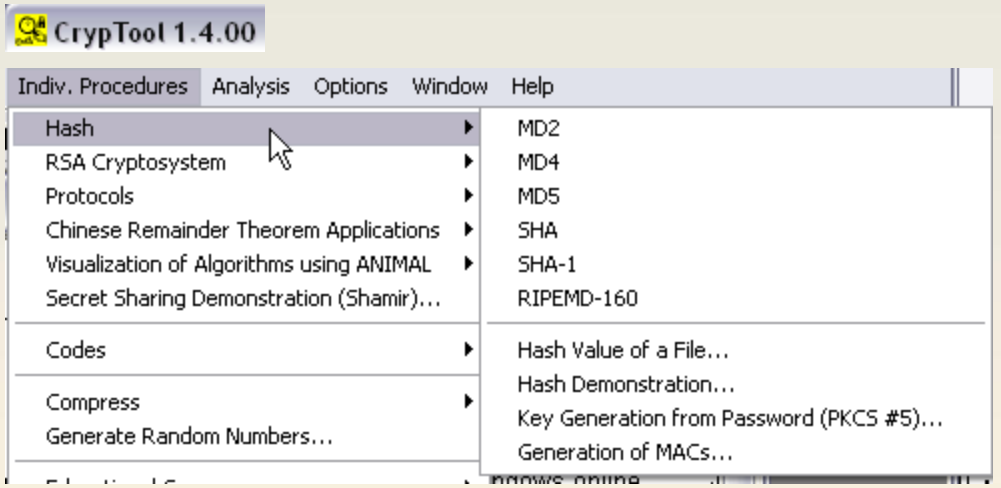


http://nsfsecurity.pr.erau.edu/crypto/generichash.html

Instructor Demonstration

Instructor will demonstrate Hashing a file using CrypTool and Express Checksum calculator.

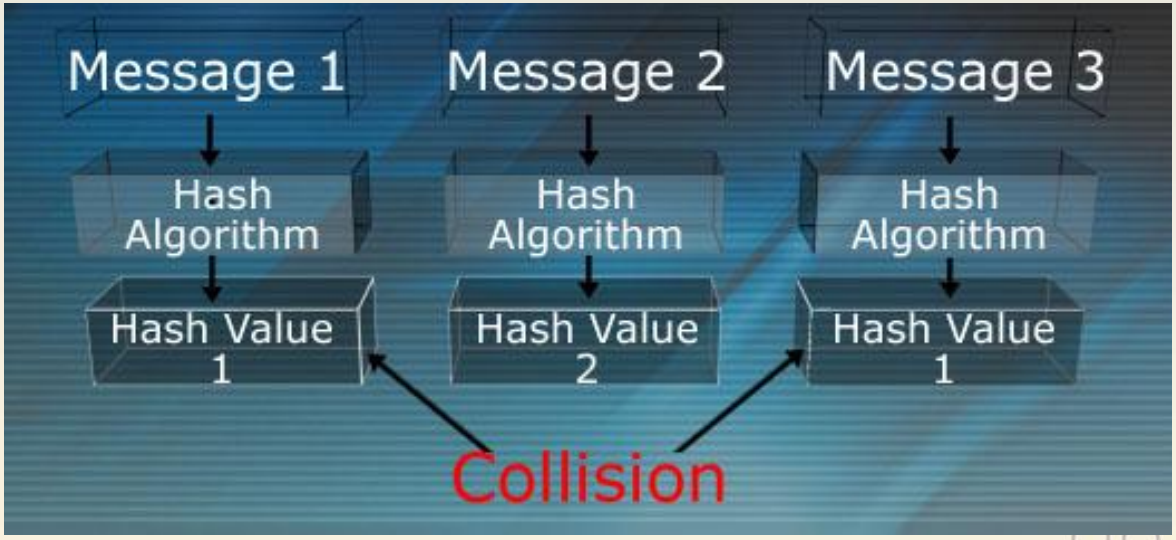




Security Issues in Hashing

Strength of Hashing Algorithms

- The hash should be computed over the entire message
- Messages cannot be disclosed by MD value
- Different messages should generate different MD values
  - Collision free
  - Resistant to birthday attacks



Hash Collisions

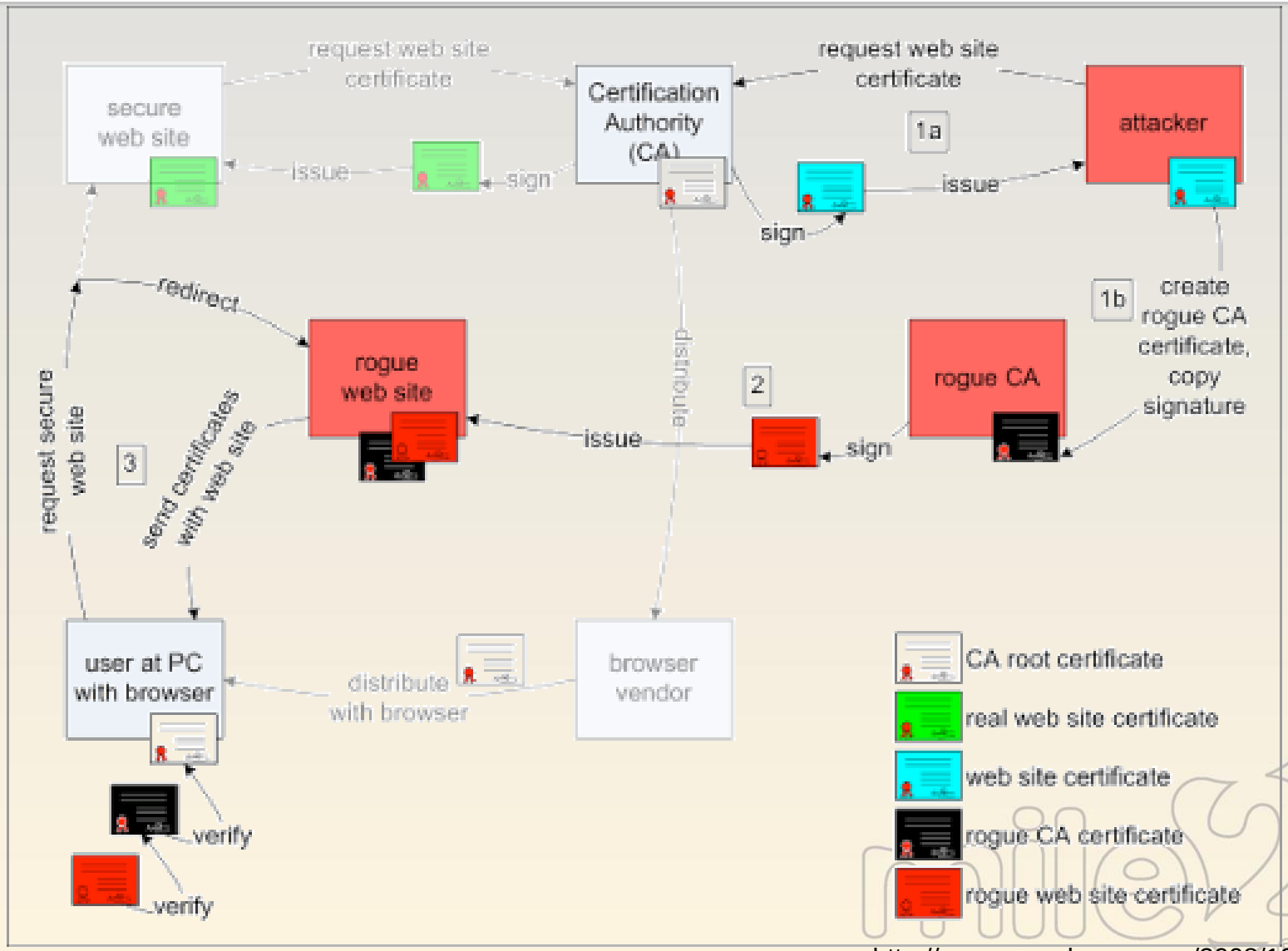
A hash collision is when two distinct data sources are input into a hashing function which then produce identical outputs.

A good hashing algorithm should minimize this potential as much as possible, to within low probability values.

Cracking the hash refers to deliberately changing the data source so that it matches a previously created hash.

This negates the integrity of the source data.

MD5 Collision Creates Rogue Certificate Authority



http://www.crunchgear.com/2008/12/30/md5-collision-creates-rogue-certificate-authority/

Hybrid Encryption

Symmetric encryption is fast, it has many algorithms available but has the problem of key management.

Asymmetric encryption is inefficient for large amounts of data but handles the key exchange in a secure manner.

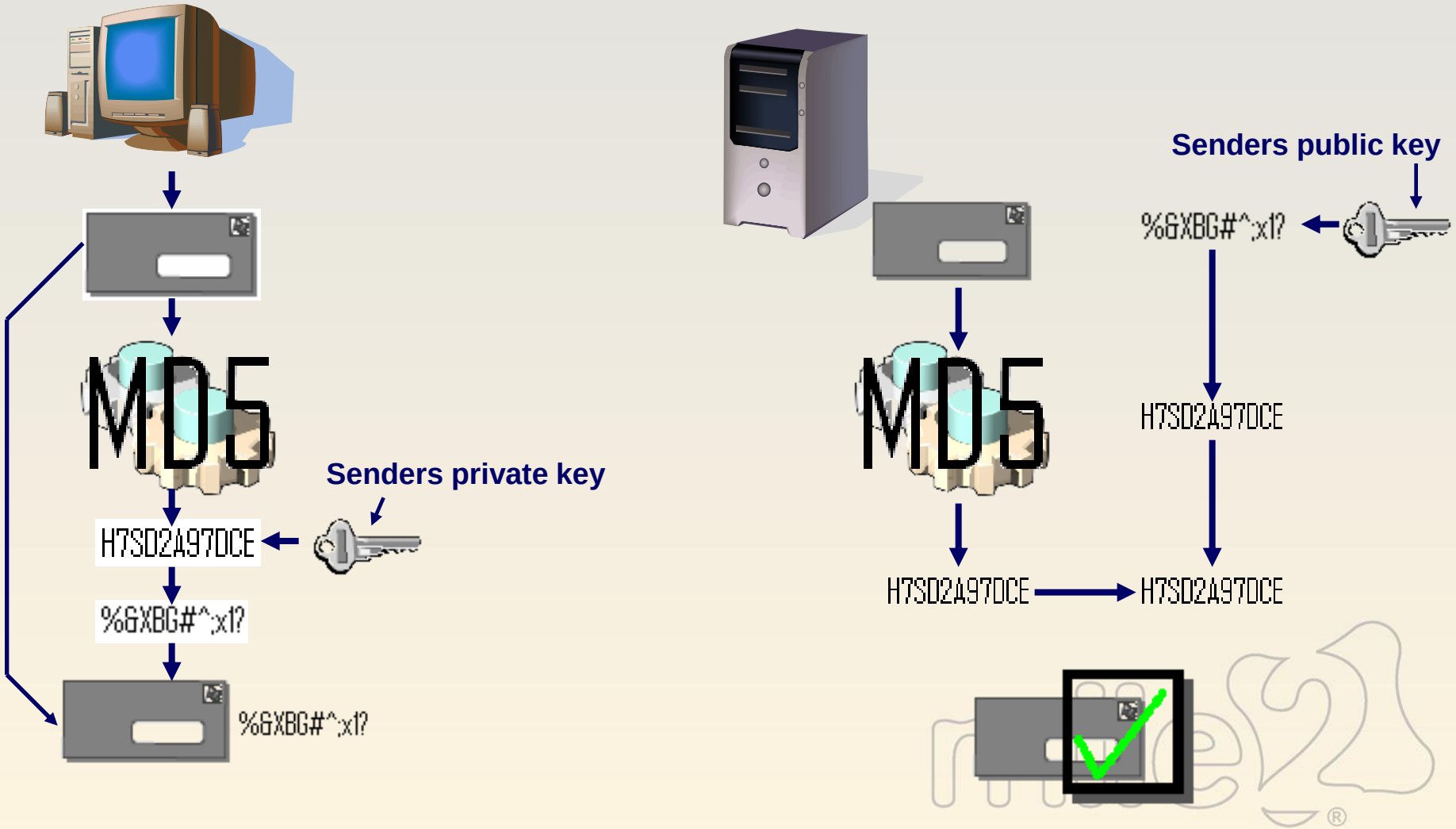
Neither allow for authentication or ensure non-repudiation.

Hybrid encryption systems bring the best of both together without the downfalls.

Hybrid encryption is very common in secure networks and even for the regular home user!

Digital Signatures

Digital signatures ensure non-repudiation.



SSL/TLS

Secure Sockets Layer (SSL) and Transport Layer Security (TLS), its successor, are cryptographic protocols which provide secure communications on the Internet for such things as e-mail, Internet faxing, and other data transfers.

SSL runs on layers beneath application protocols such as HTTP/S, FTP, SMTP and NNTP and above the TCP or UDP transport protocol.

In typical end-user/browser usage, TLS authentication is unilateral: only the server is authenticated (the client knows the server's identity), but not vice versa (the client remains unauthenticated or anonymous).

TLS also supports the more secure bilateral connection mode (typically used in enterprise applications), in which both ends of the "conversation" can be ensured with whom they are communicating (provided they diligently scrutinize the identity information in the other party's certificate). This is known as mutual authentication.

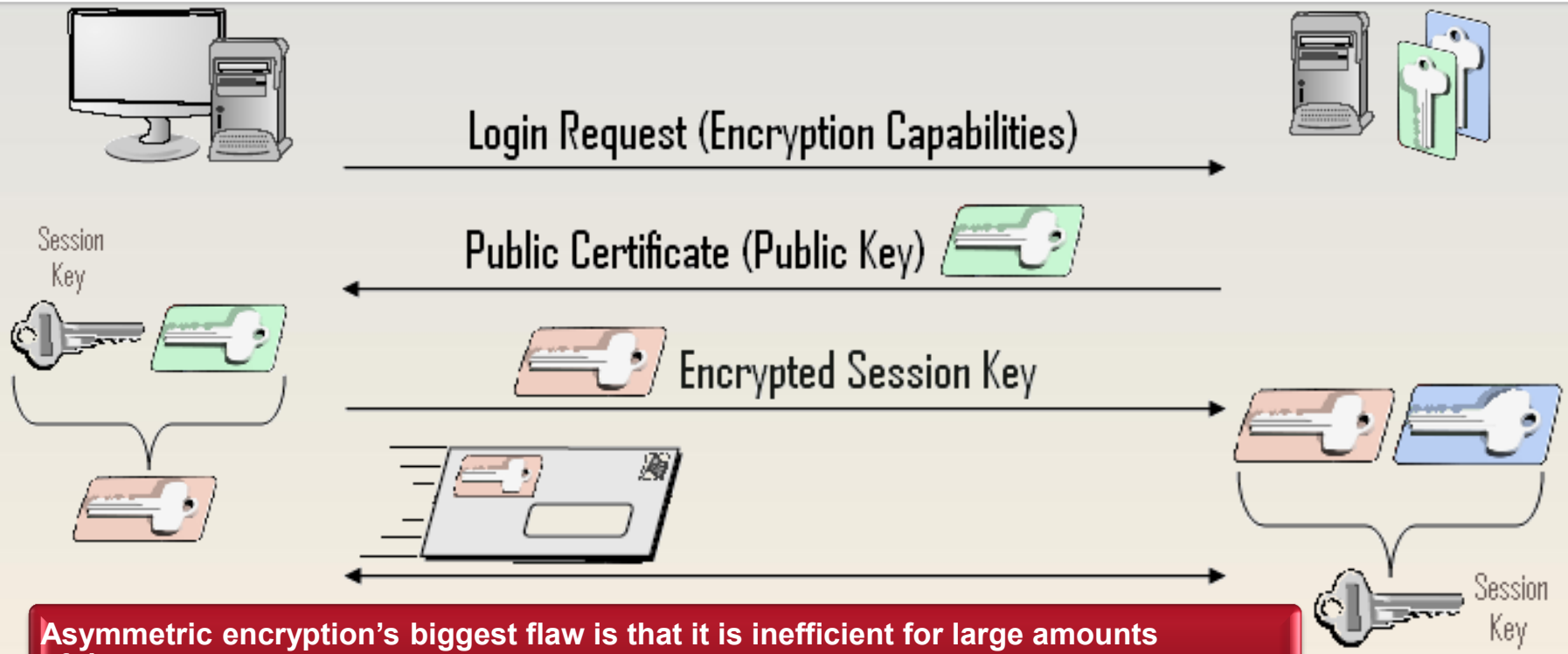
http://en.wikipedia.org/wiki/Secure_Sockets_Layer

SSL Connection Setup

Steps of Setting Up a SSL Connection

- Server sends client certificate
- Client checks to see if signing CA is in trusted list in browser
- Client computes hash of certificate and compares message digest of certificate by decrypting using CA's public key (CA signed the certificate)
- Client checks validity dates in certificate
- Client will check URL in certificate compared to URL it is communicating with
- Client extracts server's public key from certificate
- Client creates a session key (symmetric)
- Client encrypts session key with server's public key and sends it over
- Server decrypts using private key

SSL Hybrid Encryption



Asymmetric encryption's biggest flaw is that it is inefficient for large amounts of data.

Symmetric encryption's biggest flaw is the secure transfer of the key.

Some cryptography systems now use the best of both and none of the flaws.

SSH

Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

- Used primarily on Linux and Unix based systems to access shell accounts, SSH was designed as a replacement for TELNET and other insecure remote shells, which send information, notably passwords, in plaintext, leaving them open for interception.
- The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet.

SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary.[1]

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols.[1] SSH uses the client-server model.

An SSH server, by default, listens on the standard TCP port 22.[3]

An SSH client program is typically used for establishing connections to an SSH daemon accepting remote connections. Both are commonly present on most modern operating systems, including Mac OS X, Linux, FreeBSD, Solaris and OpenVMS. Proprietary, freeware and open source versions of various levels of complexity and completeness exist.

http://en.wikipedia.org/wiki/Ssh

IPSec - Network Layer Protection

IPSec

Developed because IPv4 has no security mechanisms

- Integrated in IPv6

Sets up a secure channel between computers instead of applications

- Application secure channels are usually provided with SSL

Network layer security

Can provide host-to-host, host-to-subnet, and subnet-to-subnet connections

IPSec

IPSec is a set of cryptographic protocols for securing packet flow and key exchange.

Of the former, there are two:

- **Encapsulating Security Payload (ESP) provides authentication, data confidentiality and message integrity.**
- **Authentication Header (AH) provides authentication and message integrity.**

Currently only one key exchange protocol is defined, IKE (Internet Key Exchange) protocol.

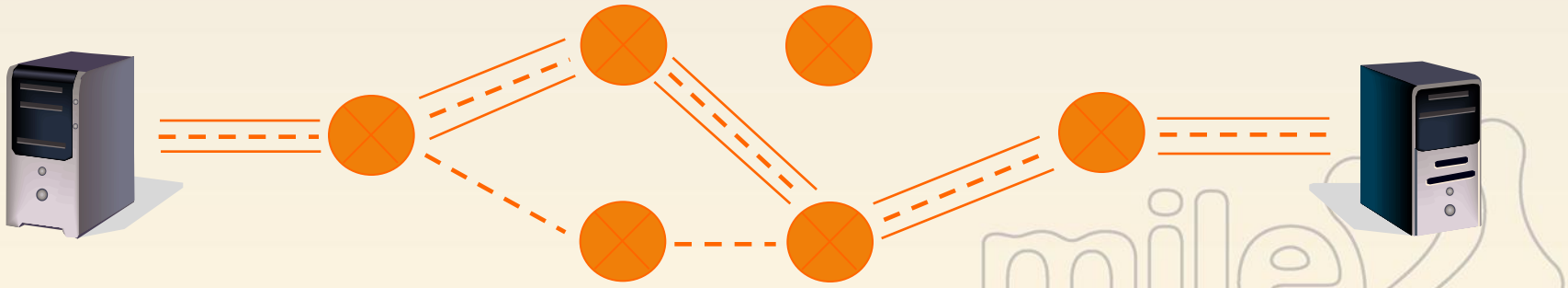
IPSec protocols operate at the network layer (layer 3 of the OSI model). Other Internet security protocols in widespread use, such as SSL and TLS, operate from the transport layer up (OSI layers 4 - 7).

IPSec

IPSec supports two encryption modes: Transport and Tunnel.

Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. Routes normally.

The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec compliant device decrypts each packet. Tunneling protocol dictates route.



Public Key Infrastructure

PKI is a user invisible system to allow for the easy usage of encryption systems and the heightened security they offer.

The main components include:

- **Certificate Authority**
- Registration Authority
- **Digital certificates**
- **Certificate revocation lists (CRL)**
- **Public key-enabled applications and services**

The building blocks are digital certificates that allow for mutual authentication and much superior encryption levels.

If a certificate is exposed to a hacker, it must be immediately revoked.

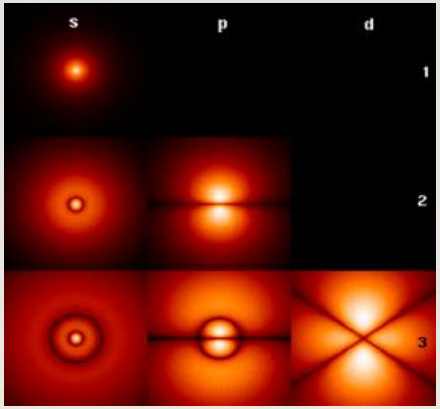
Quantum Cryptography

Quantum cryptography, or quantum key distribution (QKD), uses quantum mechanics to guarantee secure communication.

It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.

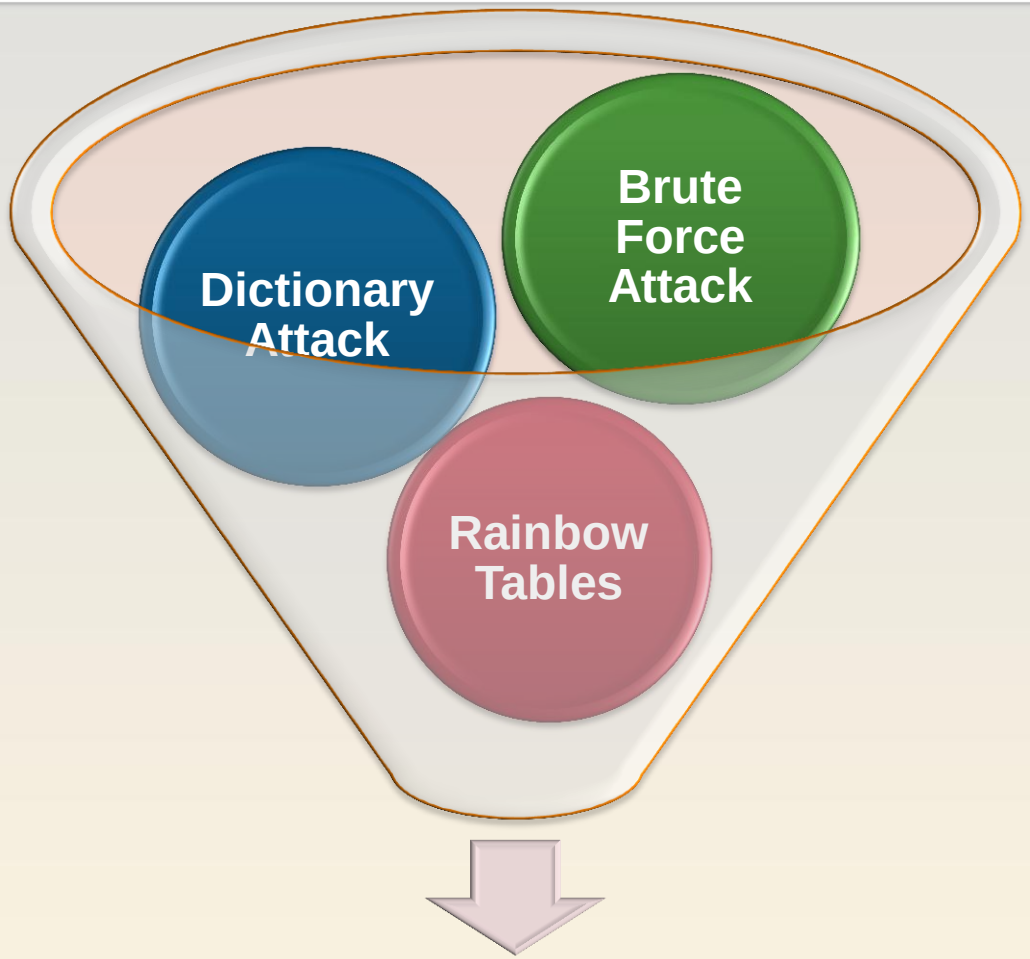
A central problem in cryptography is the key distribution problem. Public-key cryptography, relies on the computational difficulty of certain hard mathematical problems, whereas quantum cryptography relies on the laws of quantum mechanics.

Eavesdropping can be viewed as measurements on a physical object (photon/electron), in this case the carrier of the information.



Ref: http://en.wikipedia.org/wiki/Quantum_cryptography

Attack Vectors



Discovered Password

Network Attacks

Replay Attack

- Attacker obtains a set of credentials and sends them to an authentication service
  - Captures username, password, token, and ticket
- Timestamps and sequence numbers are used to protect against this attack

Man-in-the-Middle Attack

- Attacker injects itself between two users and reads messages going back and forth, or manipulates messages
- Sequence numbers and digital signatures are used to countermeasure this type of attack

More Attacks (Cryptanalysis)

Classical cryptanalysis:

- Frequency analysis
- Index of coincidence
- Kasiski examination

Symmetric algorithms:

- Boomerang attack
- Brute force attack
- Davies' attack
- Differential cryptanalysis
- Impossible differential cryptanalysis
- Integral cryptanalysis
- Linear cryptanalysis
- Meet-in-the-middle attack
- Mod-n cryptanalysis
- Related-key attack
- Slide attack
- XSL attack

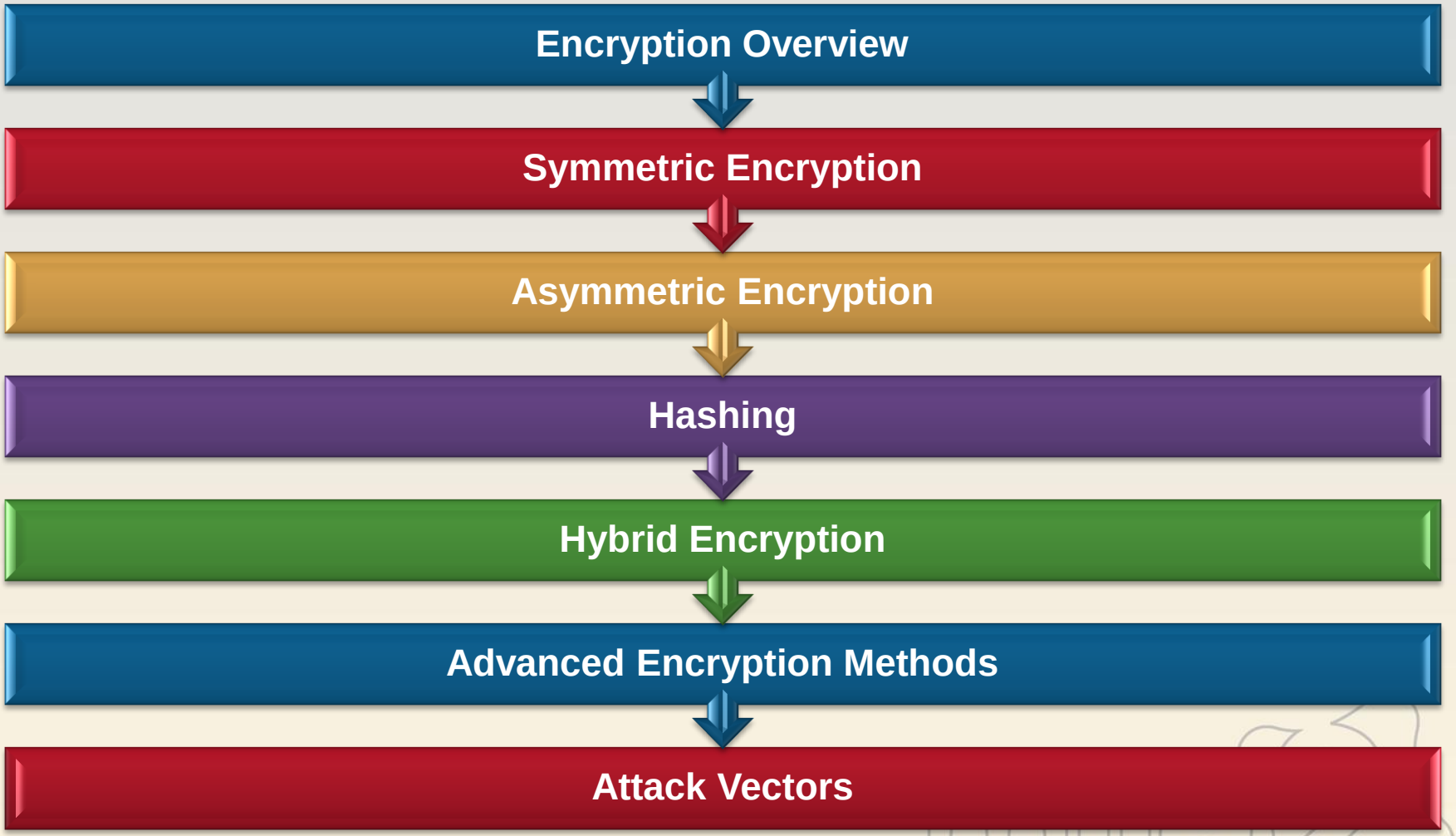
Side channel attacks:

- Power analysis
- Timing attack

External attacks:

- Black-bag cryptanalysis
- Rubber-hose cryptanalysis

Review



Case Study & Lab

Module 20 Lab
Cryptography
45 Minutes