Protecting Information Assets
- Unit# 11 -

Cryptography, Public Key Encryption and Digital Signatures
Agenda

• Cryptography and Cryptanalysis
• Terminology
• Symmetric Cryptography
• Asymmetric Cryptography
• Hashing and Digital Signature
• Public Key Infrastructure
• Cryptanalysis Attacks
• Quiz
Cryptography

• Method of transmitting and storing data in a form that only those it is intended for can read and process

• An effective way of protecting sensitive information as it is transmitted through untrusted network communication paths or stored on media

• Complements physical and logical access controls

The etymology is Greek and means: “secret writing”
Where do you look for encryption related controls?

<table>
<thead>
<tr>
<th>CLASS</th>
<th>FAMILY</th>
<th>IDENTIFIER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Risk Assessment</td>
<td>RA</td>
</tr>
<tr>
<td>Management</td>
<td>Planning</td>
<td>PL</td>
</tr>
<tr>
<td>Management</td>
<td>System and Services Acquisition</td>
<td>SA</td>
</tr>
<tr>
<td>Management</td>
<td>Certification, Accreditation, and Security Assessments</td>
<td>CA</td>
</tr>
<tr>
<td>Operational</td>
<td>Personnel Security</td>
<td>PS</td>
</tr>
<tr>
<td>Operational</td>
<td>Physical and Environmental Protection</td>
<td>PE</td>
</tr>
<tr>
<td>Operational</td>
<td>Contingency Planning</td>
<td>CP</td>
</tr>
<tr>
<td>Operational</td>
<td>Configuration Management</td>
<td>CM</td>
</tr>
<tr>
<td>Operational</td>
<td>Maintenance</td>
<td>MA</td>
</tr>
<tr>
<td>Operational</td>
<td>System and Information Integrity</td>
<td>SI</td>
</tr>
<tr>
<td>Operational</td>
<td>Media Protection</td>
<td>MP</td>
</tr>
<tr>
<td>Operational</td>
<td>Incident Response</td>
<td>IR</td>
</tr>
<tr>
<td>Operational</td>
<td>Awareness and Training</td>
<td>AT</td>
</tr>
<tr>
<td>Technical</td>
<td>Identification and Authentication</td>
<td>IA</td>
</tr>
<tr>
<td>Technical</td>
<td>Access Control</td>
<td>AC</td>
</tr>
<tr>
<td>Technical</td>
<td>Audit and Accountability</td>
<td>AU</td>
</tr>
<tr>
<td>Technical</td>
<td>System and Communications Protection</td>
<td>SC</td>
</tr>
<tr>
<td>CNTL NO.</td>
<td>CONTROL NAME</td>
<td>INITIAL CONTROL BASELINES</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td></td>
<td>System and Communications Protection Policy and Procedures</td>
<td>P1</td>
</tr>
<tr>
<td>SC-2</td>
<td>Application Partitioning</td>
<td>P1</td>
</tr>
<tr>
<td>SC-3</td>
<td>Security Function Isolation</td>
<td>P1</td>
</tr>
<tr>
<td>SC-4</td>
<td>Information in Shared Resources</td>
<td>P1</td>
</tr>
<tr>
<td>SC-5</td>
<td>Denial of Service Protection</td>
<td>P1</td>
</tr>
<tr>
<td>SC-6</td>
<td>Resource Availability</td>
<td>P0</td>
</tr>
<tr>
<td>SC-7</td>
<td>Boundary Protection</td>
<td>P1</td>
</tr>
<tr>
<td>SC-8</td>
<td>Transmission Confidentiality and Integrity</td>
<td>P1</td>
</tr>
<tr>
<td>SC-9</td>
<td>Withdrawed</td>
<td>---</td>
</tr>
<tr>
<td>SC-10</td>
<td>Network Disconnect</td>
<td>P2</td>
</tr>
<tr>
<td>SC-11</td>
<td>Trusted Path</td>
<td>P0</td>
</tr>
<tr>
<td>SC-12</td>
<td>Cryptographic Key Establishment and Management</td>
<td>P1</td>
</tr>
<tr>
<td>SC-13</td>
<td>Cryptographic Protection</td>
<td>P1</td>
</tr>
<tr>
<td>SC-14</td>
<td>Withdrawed</td>
<td>---</td>
</tr>
<tr>
<td>SC-16</td>
<td>Transmission of Security Attributes</td>
<td>P0</td>
</tr>
<tr>
<td>SC-17</td>
<td>Public Key Infrastructure Certificates</td>
<td>P1</td>
</tr>
<tr>
<td>SC-19</td>
<td>Voice Over Internet Protocol</td>
<td>P1</td>
</tr>
<tr>
<td>SC-20</td>
<td>Secure Name (Address Resolution Service (Authority Source))</td>
<td>P1</td>
</tr>
<tr>
<td>SC-21</td>
<td>Secure Name (Address Resolution Service (Recursive or Caching Resolver))</td>
<td>P1</td>
</tr>
<tr>
<td>SC-22</td>
<td>Architecture and Provisioning for Name/Address Resolution Service</td>
<td>P1</td>
</tr>
<tr>
<td>SC-23</td>
<td>Session Authenticity</td>
<td>P1</td>
</tr>
<tr>
<td>SC-24</td>
<td>Fall in Known State</td>
<td>P1</td>
</tr>
<tr>
<td>SC-28</td>
<td>Protection of Information at Rest</td>
<td>P1</td>
</tr>
</tbody>
</table>

**SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**

**Control:** The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

**Supplemental Guidance:** Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems. Related controls: SC-13, SC-17.

**Control Enhancements:**

1. **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY**
   - The organization maintains availability of information in the event of the loss of cryptographic keys by users.
   - **Supplemental Guidance:** Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).

2. **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS**
   - The organization produces, controls, and distributes symmetric cryptographic keys using [Selection: NIST FIPS-compliant; NSA-approved] key management technology and processes.

3. **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS**
   - The organization produces, controls, and distributes asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user’s private key].

4. **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES**
   - [Withdrawn: Incorporated into SC-12].

5. **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS**
   - [Withdrawn: Incorporated into SC-12].

**References:** NIST Special Publications 800-56, 800-57.

**Priority and Baseline Allocation:**

- P1 LOW SC-12
- MOD SC-12
- HIGH SC-12 (1)
<table>
<thead>
<tr>
<th>SC-1</th>
<th>System and Communications Protection Policy and Procedures</th>
<th>P1</th>
<th>SC-1</th>
<th>SC-1</th>
<th>SC-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC-2</td>
<td>Application Partitioning</td>
<td>P1</td>
<td>Not Selected</td>
<td>SC-2</td>
<td>SC-2</td>
</tr>
<tr>
<td>SC-3</td>
<td>Security Function Isolation</td>
<td>P1</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>SC-3</td>
</tr>
<tr>
<td>SC-4</td>
<td>Information in Shared Resources</td>
<td>P1</td>
<td>Not Selected</td>
<td>SC-4</td>
<td>SC-4</td>
</tr>
<tr>
<td>SC-5</td>
<td>Denial of Service Protection</td>
<td>P1</td>
<td>SC-5</td>
<td>SC-5</td>
<td>SC-5</td>
</tr>
<tr>
<td>SC-6</td>
<td>Resource Availability</td>
<td>P0</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
</tr>
<tr>
<td>SC-7</td>
<td>Boundary Protection</td>
<td>P1</td>
<td>SC-7</td>
<td>SC-7 (3) (4) (5) (7)</td>
<td>SC-7 (3) (4) (5) (7) (8) (18) (21)</td>
</tr>
<tr>
<td>SC-8</td>
<td>Transmission Confidentiality and Integrity</td>
<td>P1</td>
<td>Not Selected</td>
<td>SC-8 (1)</td>
<td>SC-8 (1)</td>
</tr>
<tr>
<td>SC-9</td>
<td>Withdrawn</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>SC-10</td>
<td>Network Disconnect</td>
<td>P2</td>
<td>Not Selected</td>
<td>SC-10</td>
<td>SC-10</td>
</tr>
<tr>
<td>SC-11</td>
<td>Trusted Path</td>
<td>P0</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
</tr>
<tr>
<td>SC-12</td>
<td>Cryptographic Key Establishment and Management</td>
<td>P1</td>
<td>SC-12</td>
<td>SC-12</td>
<td>SC-12 (1)</td>
</tr>
<tr>
<td>SC-13</td>
<td>Cryptographic Protection</td>
<td>P1</td>
<td>SC-13</td>
<td>SC-13</td>
<td>SC-13</td>
</tr>
<tr>
<td>SC-14</td>
<td>Withdrawn</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>SC-16</td>
<td>Transmission of Security Attributes</td>
<td>P0</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
</tr>
<tr>
<td>SC-17</td>
<td>Public Key Infrastructure Certificates</td>
<td>P1</td>
<td>Not Selected</td>
<td>SC-17</td>
<td>SC-17</td>
</tr>
<tr>
<td>SC-18</td>
<td>Mobile Code</td>
<td>P2</td>
<td>Not Selected</td>
<td>SC-18</td>
<td>SC-18</td>
</tr>
<tr>
<td>SC-19</td>
<td>Voice Over Internet Protocol</td>
<td>P1</td>
<td>SC-19</td>
<td>SC-19</td>
<td>SC-19</td>
</tr>
<tr>
<td>SC-20</td>
<td>Secure Name Address Resolution Service (Authoritative Source)</td>
<td>P1</td>
<td>SC-20</td>
<td>SC-20</td>
<td>SC-20</td>
</tr>
<tr>
<td>SC-21</td>
<td>Secure Name Address Resolution Service (Recursive or Caching Resolver)</td>
<td>P1</td>
<td>SC-21</td>
<td>SC-21</td>
<td>SC-21</td>
</tr>
<tr>
<td>SC-22</td>
<td>Architecture and Provisioning for Name Address Resolution Service</td>
<td>P1</td>
<td>SC-22</td>
<td>SC-22</td>
<td>SC-22</td>
</tr>
<tr>
<td>SC-23</td>
<td>Session Authenticity</td>
<td>P1</td>
<td>Not Selected</td>
<td>SC-23</td>
<td>SC-23</td>
</tr>
<tr>
<td>SC-24</td>
<td>Fall in Known State</td>
<td>P1</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>SC-24</td>
</tr>
<tr>
<td>SC-28</td>
<td>Protection of Information at Rest</td>
<td>P1</td>
<td>Not Selected</td>
<td>SC-28</td>
<td>SC-28</td>
</tr>
</tbody>
</table>

### SC-13 CRYPTOGRAPHIC PROTECTION

**Control:** The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

**Supplemental Guidance:** Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

**Control Enhancements:** None.

1. **CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY**  
   [Withdrawn: Incorporated into SC-13].

2. **CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY**  
   [Withdrawn: Incorporated into SC-13].

3. **CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS**  
   [Withdrawn: Incorporated into SC-13].

4. **CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES**  
   [Withdrawn: Incorporated into SC-13].


**Priority and Baseline Allocation:**

<table>
<thead>
<tr>
<th>P1</th>
<th>LOW SC-13</th>
<th>MOD SC-13</th>
<th>HIGH SC-13</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC-13</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cryptanalysis

- The study of methods to break cryptosystems
- Often targeted at obtaining a key
- Attacks may be passive or active

- Kerckhoff’s Principle
  - The only secrecy involved with a cryptosystem should be the key

- Cryptosystem Strength
  - How hard is it to determine the secret associated with the system?
Terminology

- **Plaintext** – is the readable version of a message
- **Ciphertext** – is the unreadable results after an encryption process is applied to the plaintext
- **Cryptosystem** – includes all the necessary components for encryption and decryption
  - Algorithms
  - Keys
  - Software
  - Protocols

Services of cryptosystems

• **Confidentiality** – Renders information unintelligible except by authorized entities

• **Integrity** – Data has not been altered in an unauthorized manner since it was created, transmitted, or stored

• **Authentication** – Verifies the identity of the user or system that created, requested or provided the information
  - • **Authorization** – *On proving identity, the individual is provided with the key or password that will permit access to some resource*

• **Nonrepudiation** – Ensure the sender cannot deny sending the information

  *Repudiation – the sender denying he sent the message*

Cipher = encryption algorithm
2 main attributes combined in a cypher

1. **Confusion**: usually carried out through substitution

2. **Diffusion**: Usually carried out through transposition
Cipher = encryption algorithm
2 main attributes combined in a cypher

1. **Confusion**: usually carried out through substitution

2. **Diffusion**: Usually carried out through transposition
Example: Substitution cipher or algorithm

- A mono-alphabetic substitution cipher
  
  $\text{ABCDEFHIJKLMNOPQRSTUVWXYZ}$
  $\text{ZYZXWVUTSRQPONMLKJIHGFEDCBA}$

  “SECURITY” $\leftrightarrow$ “HVXFIRGB”

- Poly-alphabetic substitution cipher

  - **Standard Alphabet:**
    $\text{ABCDEFGHIJKLMNOPQRSTUVWXYZ}$
  
  - **Cryptographic Alphabet:**
    $\text{DEFGHIJKLMNOPQRSTUVWXYZABC}$

  - **Plaintext:**
    LOGICAL SECURITY

  - **Ciphertext:**
    ORJLFDO VHFXULWB
Cipher Disk

Outer wheel is for the *plaintext* alphabet
Inner wheel is for *ciphertext*

When the outer wheel and inner wheel and are both aligned at the letter “A” (i.e. position zero), there is no encryption mapping the letters on the outer wheel to letters on the inner wheel.
Secret
Keyspace is the number of possible keys
Question B: Assuming each key is equally likely (randomly distributed) how many random guesses would you have to make on average to find the key to decrypt the plaintext?

Answer: \(~14\), \((28 - 1) = 27\) and \(27/2 = 13.5\) which is approximately \(14\)

- Because the _average_ of a uniform distribution is half
- Recall 26 letters in the alphabet + “.” and “-” = 28, but we cannot use “0” as the key which gives us the original plaintext back the size of the alphabet

- This is important in cryptography because _on average_ the number of attempts needed to successfully guess the key through brute forcing is half of the key space
- This is true of the simple cipher wheel as well as modern encryption schemes with very large key spaces
Linguistic cryptanalysis examples...

• Recognizing the beginning of the word
• Looking for letter pairs
• Looking at vowels

This form of cryptanalysis uses your knowledge of the English language
Linguistic cryptanalysis examples...

One form of linguistic cryptanalysis is frequency analysis of letters used in English.

Frequency analysis recognizes that different letters have different probabilities of frequencies of use in words:

Given a sentence written in the English language:
- E, T, A and O are the most common.
- Z, Q and X are rare.
- TH, ER, ON, and AN are the most common pairs of letters (termed bigrams or digraphs).
- SS, EE, TT, and FF are the most common repeats.
Example: Substitution cipher or algorithm

- **Standard Alphabet:**
  
  ABCDEFGHIJKLMNOPQRSTUVWXYZ

- **Cryptographic Alphabet:**
  
  DEFGHIJKLMNOPQRSTUVWXYZABC

- **Plaintext:**
  LOGICAL SECURITY

- **Ciphertext:**
  ORJLFDO VHFXULWB
Polyalphabetic Cipher

Ciphers can be made stronger, and frequency analysis made more difficult when more than one cipher alphabet is used

• For example, encrypt the plaintext message “SEND MONEY”
  • Use the word “SECURITY” as the key, but repeat its use in the key to make it have as many letters as the plaintext:

Plaintext: SEND MONEY (10 characters including the space “_”)
  Key: SECURITYYSE (10 characters)

1. Encrypt by rotating the inner wheel so that “s” in the word “security” aligns with “a” on the outer wheel. Now “s” in the word “send” on the outer wheel maps to the letter “i” on the inner wheel, so “i” is the ciphertext.
Polyalphabetic Cipher

Plaintext: SEND MONEY (10 characters including the space “_”)
Key: SECURITYSE (10 characters)

1. Encrypt by rotating the inner wheel so that “S” in the word “SECURITY” aligns with “A” on the outer wheel. Now “S” in the word “SEND” on the outer wheel maps to the letter “I” on the inner wheel, so “I” is the ciphertext.

2. Next, rotate the inner wheel so that “E” in the word “SECURITY” aligns with “A” on the outer wheel. Now “E” in the word “SEND” on the outer wheel maps to “I” on the inner wheel, so “I” is the ciphertext again, even though the plaintext is different than before.

Question: What is the rest of the ciphertext for “SEND MONEY” using the polyalphabetic key “SECURITY”? IIPXPUFJWA

Polyalphabetic ciphers make frequency analysis more difficult.

Polyalphabetic substitution is another building block of cryptography.
Random Polyalphabetic Cipher

What if we use a random polyalphabetic key that is as long as the message?

For example, let’s say our plaintext is:

*We intend to begin on the first of February unrestricted submarine warfare.*

And the polyalphabetic key is a string of random characters as long as the message:

*ackwulsjwkbogbzcuqk.qubpnnefjvcebuymacizvzmzwfbxpmzmzqwm*  
*mejzf*

**Question:** How would an attacker could attempt to crack this message?  
Is an attack possible?
Cipher = encryption algorithm
2 main attributes combined in a cypher

1. **Confusion:** usually carried out through substitution
   • *Let’s look at another way to do substitution*

2. **Diffusion:** Usually carried out through transposition
Binary – Decimal

0 0 0 0 0 0 0 0 0 = 0
1 1 1 1 1 1 1 1 1 = 255

8 bits supports 256 numbers

Decimal - ASCII

ASCII Character Table

<table>
<thead>
<tr>
<th>Name</th>
<th>Hex</th>
<th>Dec</th>
</tr>
</thead>
<tbody>
<tr>
<td>. (period)</td>
<td>2E</td>
<td>046</td>
</tr>
<tr>
<td>0</td>
<td>30</td>
<td>048</td>
</tr>
<tr>
<td>1</td>
<td>31</td>
<td>049</td>
</tr>
<tr>
<td>2</td>
<td>32</td>
<td>050</td>
</tr>
<tr>
<td>3</td>
<td>33</td>
<td>051</td>
</tr>
<tr>
<td>4</td>
<td>34</td>
<td>052</td>
</tr>
<tr>
<td>5</td>
<td>35</td>
<td>053</td>
</tr>
<tr>
<td>6</td>
<td>36</td>
<td>054</td>
</tr>
<tr>
<td>7</td>
<td>37</td>
<td>055</td>
</tr>
<tr>
<td>8</td>
<td>38</td>
<td>056</td>
</tr>
<tr>
<td>9</td>
<td>39</td>
<td>057</td>
</tr>
<tr>
<td>A</td>
<td>41</td>
<td>065</td>
</tr>
<tr>
<td>B</td>
<td>42</td>
<td>066</td>
</tr>
<tr>
<td>C</td>
<td>43</td>
<td>067</td>
</tr>
<tr>
<td>D</td>
<td>44</td>
<td>068</td>
</tr>
<tr>
<td>E</td>
<td>45</td>
<td>069</td>
</tr>
<tr>
<td>F</td>
<td>46</td>
<td>070</td>
</tr>
<tr>
<td>G</td>
<td>47</td>
<td>071</td>
</tr>
<tr>
<td>H</td>
<td>48</td>
<td>072</td>
</tr>
<tr>
<td>I</td>
<td>49</td>
<td>073</td>
</tr>
<tr>
<td>J</td>
<td>4A</td>
<td>074</td>
</tr>
<tr>
<td>K</td>
<td>4B</td>
<td>075</td>
</tr>
<tr>
<td>L</td>
<td>4C</td>
<td>076</td>
</tr>
<tr>
<td>M</td>
<td>4D</td>
<td>077</td>
</tr>
<tr>
<td>N</td>
<td>4E</td>
<td>078</td>
</tr>
<tr>
<td>O</td>
<td>4F</td>
<td>079</td>
</tr>
<tr>
<td>P</td>
<td>50</td>
<td>080</td>
</tr>
<tr>
<td>Q</td>
<td>51</td>
<td>081</td>
</tr>
<tr>
<td>R</td>
<td>52</td>
<td>082</td>
</tr>
<tr>
<td>S</td>
<td>53</td>
<td>083</td>
</tr>
<tr>
<td>T</td>
<td>54</td>
<td>084</td>
</tr>
<tr>
<td>U</td>
<td>55</td>
<td>085</td>
</tr>
<tr>
<td>V</td>
<td>56</td>
<td>086</td>
</tr>
<tr>
<td>W</td>
<td>57</td>
<td>087</td>
</tr>
<tr>
<td>X</td>
<td>58</td>
<td>088</td>
</tr>
<tr>
<td>Y</td>
<td>59</td>
<td>089</td>
</tr>
<tr>
<td>Z</td>
<td>5A</td>
<td>090</td>
</tr>
</tbody>
</table>
Creating “confusion” through a binary mathematical function called “exclusive OR”, abbreviated as XOR

- **Message stream:** 1001010111
- **Keystream:** 0011101010
- **Ciphertext stream:** 1010111101

One-Time Pad  *a perfect encryption scheme*

One-Time Pad Requirements

- Made up of truly random values
- Used only one time
- Securely distributed to its destination
- Secured at sender’s and receiver’s sites
- At least as long as the message

One-time pad -- Problems

• Must be *perfectly* random
• Pad must be as long as the message
• **Must be used only once**
  • Skimp on any of these conditions, it becomes trivial to break your system
• Any software product claiming to use one-time pad is **snake-oil**.
  • Computers are bad at generating *truly* random numbers
Cipher = encryption algorithm
2 main attributes combined in a cypher

1. **Confusion:** usually carried out through substitution

2. **Diffusion:** Usually carried out through transposition

Transposition

- Ancient example: *scytale*
A profit was achieved by our ACT unit
A profit was achieved by our act unit
A profit was achieved by our act unit.
6025487139
tarifawpos
eahvedciy
uortcinuat
0123456789

A profit was achieved by our act unit
2 main attributes combined in a cypher

1. **Confusion**: usually carried out through substitution

2. **Diffusion**: Usually carried out through transposition

---

Examples of dichotomies in cryptography

• Symmetric versus Asymmetric
• Stream versus block
• 1-Way functions versus 2-Way functions
Symmetric versus asymmetric algorithms

• **Symmetric cryptography**
  • Use a copied pair of symmetric (identical) secret keys
  • The sender and the receive use the same key for encryption and decryption functions

• **Asymmetric cryptography**
  • Also know as “public key cryptography”
  • Use different ("asymmetric") keys for encryption and decryption
  • One is called the “private key” and the other is the “public key”
Symmetric cryptography

Strengths:
- Much faster (less computationally intensive) than asymmetric systems.
- Hard to break if using a large key size.

Weaknesses:
- Requires a secure mechanism to deliver keys properly.
- Each pair of users needs a unique key, so as the number of individuals increases, so does the number of keys, possibly making key management overwhelming.
- Provides confidentiality but not authenticity or nonrepudiation.

Two types: Stream and Block Ciphers

- **Stream Ciphers** treat the message a stream of bits and performs mathematical functions on each bit individually
- **Block Ciphers** divide a message into blocks of bits and transforms the blocks one at a time
Symmetric Stream Ciphers

- Easy to implement in hardware
- Used in cell phones and Voice Over Internet Protocol

Symmetric versus asymmetric algorithms

• Symmetric cryptography
  • Use a copied pair of symmetric (identical) secret keys
  • The sender and the receive use the same key for encryption and decryption functions

• Asymmetric cryptography
  • Also know as “public key cryptography”
  • Use different (“asymmetric”) keys for encryption and decryption
  • One is called the “private key” and the other is the “public key”
Asymmetric cryptography

- **Public and Private** keys are mathematically related
  - Public keys are generated from private key
  - Private keys cannot be derived from the associated public key (if it falls into the wrong hands)

- **Public key** can be known by everyone
- **Private key** must be known and used only by the owner

Asymmetric systems use two different keys for encryption and decryption purposes.

Asymmetric cryptography is computational intensive and much slower than symmetric cryptography

Asymmetric cryptography

• Do not get confused and think the public key is only for encryption and private key is only for decryption!

• Each key type can be used to encrypt and decrypt
  • If data is encrypted with a private key it cannot be decrypted with the same private key (but it can be decrypted with the related public key)
  • If data is encrypted with a public key it cannot be decrypted with the same public key (but it can be decrypted with the related private key)
Asymmetric cryptography

If the sender ("Jill") encrypts data with her private key, the receiver ("Bill") must have a copy of Jill’s public key to decrypt it

• By decrypting the message with Jill’s public key Bill can be sure the message really came from Jill
• A message can be decrypted with a public key only if the message was encrypted with the corresponding private key
  • *This provides authentication because Jill is only the only one who is supposed to have her private key*

If Bill (the receiver) wants to make sure Jill is the only one who can read his reply, he will encrypt the response with her public key

  – *Only Jill will be able to decrypt the message, because she is the only one who has the necessary private key*
  – *This provides confidentiality because only Jill is able to decrypt the message with her private key*
Asymmetric cryptography

Why would Bill (now the sender) choose to encrypt his reply to Jill with his private key instead of using Jill’s public key?

- **Authentication** – Bill wants Jill to know that the message came from him and no one else
- If he encrypted the data with Jill’s public key, it does not provide authenticity because anyone can get Jill’s public key
- If he uses his private key to encrypt the data, then Jill can be sure the message came from him and no one else

*Note:* Symmetric keys do not provide authenticity – because the same key is used on both ends (using one of the secret keys does not ensure the message originated from a specific individual)
Asymmetric cryptography

• If **confidentiality** is the most important security service, the sender would encrypt the file with the receiver’s public key
  • This is called a “**secure message format**” because it can only be decrypted by the person with the corresponding private key

• If **authentication** is most important, the sender would encrypt the data with his private key
  – This provides assurance to the receiver that the only person who could have encrypted the data is the individual in possession of the private key
  – If the sender encrypted the data with receivers public key, authentication is not provided because the public key is available to anyone
  – Encrypting data with the senders private key is called an “**open message format**” because anyone with a copy of the corresponding public key can decrypt the message
  – **Confidentiality is not assured**
Elliptical curve cryptography (ECC) is a public key encryption technique (Asymmetric)
• Based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys
• ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers
Hybrid Encryption (a.k.a. “digital envelope”)

Symmetric and asymmetric algorithms are often used together

• Public key cryptography’s asymmetric algorithm is used to create public and private keys for secure automated key distribution

• Symmetric algorithm is used to create secret keys for rapid encryption/decryption of bulk data

Public Key Management

Figure 9.1 Public-Key Cryptography

Hybrid Encryption

Symmetric algorithm uses a secret key to encrypt the message and the asymmetric key encrypts the secret key for transmission (SSL/TLS uses hybrid)

Quick review

1. If a symmetric key is encrypted with a receiver’s public key, what security service is provided?
Quick review

1. If a symmetric key is encrypted with a receiver’s public key, what security service is provided?
   
   • **Confidentiality**: only the receiver’s private key can be used to decrypt the symmetric key, and only the receiver should have access to this private key
Quick review

2. If data is encrypted with the sender’s private key, what security services is provided?
Quick review

2. If data is encrypted with the sender’s private key, what security services are provided?
   • **Authenticity** of the sender and nonrepudiation. If the receiver can decrypt the encrypted data with the sender’s public key, then receiver knows the data was encrypted with the sender’s private key.
Quick review

3. Why do we encrypt the message with the symmetric key rather than the asymmetric key?
Quick review

3. Why do we encrypt the message with the symmetric key rather than the asymmetric key?
   - Because the asymmetric key algorithm is too slow
Session keys

Single-use symmetric keys used to encrypt messages between two users in an individual communication session

1) Tanya sends Lance her public key.
2) Lance generates a random session key and encrypts it using Tanya’s public key.
3) Lance sends the session key, encrypted with Tanya’s public key, to Tanya.
4) Tanya decrypts Lance’s message with her private key and now has a copy of the session key.
5) Tanya and Lance use this session key to encrypt and decrypt messages to each other.

This is how secure web client applications communicate with server-side services
One-way Hash

- Assures message **integrity**
- A function that takes a variable-length string (i.e. message) and produces a fixed-length value called a hash value
- Does not use keys

1. Sender puts message through hashing function
2. Message digest generated
3. Message digest appended to the message
4. Sender sends message to receiver
5. Receiver puts message through hashing function
6. Receiver generates message digest value
7. Receiver compares the two message digests values. If they are the same, the message has not been altered
One-way hash example...

*Testing the integrity of a file (e.g. program) downloaded from the internet...*
One-way hash example...

Testing the integrity of a file (e.g. program) from the internet...

<table>
<thead>
<tr>
<th>Image Name</th>
<th>Download</th>
<th>Size</th>
<th>Version</th>
<th>sha256sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kali 64 bit</td>
<td>HTTP</td>
<td>2.8G</td>
<td>2017.2</td>
<td>4556775bf981ae64a3cb19a0b73e8dcac6e4ba524f31c4bc14c9137b99725d</td>
</tr>
</tbody>
</table>

Is the Kali I downloaded the same Kali that was published?
One-way hash example...
One-way hash example...

https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-5.1

Example 1: Compute the hash value for a PowerShell.exe file

```
PS C:\> Get-FileHash $pshome\powershell.exe | Format-List
Algorithm : SHA256
Hash      : 6A785AD0C826338DAB3EB3F8C185C8FBA77EB5D425D0834CA864F1BE1C8B73
Path      : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

This command uses the **Get-FileHash** cmdlet to compute the hash value for the Powershell.exe file. The hash algorithm used is the default, SHA256. The output is piped to the Format-List cmdlet to format the output as a list.
```bash
PS C:\Users\tue87168> dir

Directory: C:\Users\tue87168

<table>
<thead>
<tr>
<th>Mode</th>
<th>LastWriteTime</th>
<th>Length Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>d----</td>
<td>9/27/2016 11:28 AM</td>
<td>.oracle_fce_usage</td>
</tr>
<tr>
<td>d----</td>
<td>6/21/2016 10:57 AM</td>
<td>Benefits</td>
</tr>
<tr>
<td>d----</td>
<td>10/13/2017 8:35 AM</td>
<td>Contacts</td>
</tr>
<tr>
<td>d----</td>
<td>11/5/2017 8:48 PM</td>
<td>Desktop</td>
</tr>
<tr>
<td>d----</td>
<td>11/7/2017 8:52 AM</td>
<td>Documents</td>
</tr>
<tr>
<td>d----</td>
<td>11/9/2017 2:51 PM</td>
<td>Downloads</td>
</tr>
<tr>
<td>d----</td>
<td>10/13/2017 8:35 AM</td>
<td>Favorites</td>
</tr>
<tr>
<td>d----</td>
<td>11/6/2017 9:33 AM</td>
<td>Google Drive</td>
</tr>
<tr>
<td>d----</td>
<td>11/7/2017 2:53 PM</td>
<td>Intel</td>
</tr>
<tr>
<td>d----</td>
<td>11/2/2017 8:16 AM</td>
<td>Wives</td>
</tr>
<tr>
<td>d----</td>
<td>6/20/2017 5:07 PM</td>
<td>Togs</td>
</tr>
<tr>
<td>d----</td>
<td>8/10/2016 10:08 AM</td>
<td>Music</td>
</tr>
<tr>
<td>d----</td>
<td>10/13/2017 8:35 AM</td>
<td>OneDrive</td>
</tr>
<tr>
<td>d----</td>
<td>11/2/2017 8:16 AM</td>
<td>Pictures</td>
</tr>
<tr>
<td>d----</td>
<td>6/9/2017 11:20 AM</td>
<td>Rooming</td>
</tr>
<tr>
<td>d----</td>
<td>10/13/2017 8:35 AM</td>
<td>Saved Games</td>
</tr>
<tr>
<td>d----</td>
<td>10/13/2017 8:35 AM</td>
<td>Searches</td>
</tr>
<tr>
<td>d----</td>
<td>11/17/2017 11:20 AM</td>
<td>Tracing</td>
</tr>
<tr>
<td>d----</td>
<td>10/13/2017 8:35 AM</td>
<td>Videos</td>
</tr>
</tbody>
</table>

PS C:\Users\tue87168> cd Downloads
PS C:\Users\tue87168> dir -q iso

Directory: C:\Users\tue87168\Downloads

<table>
<thead>
<tr>
<th>Mode</th>
<th>LastWriteTime</th>
<th>Length Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>a-----</td>
<td>8/10/2017 10:55 AM</td>
<td>674803712 CentOS 7.4 (1).iso</td>
</tr>
<tr>
<td>a-----</td>
<td>8/10/2017 11:03 AM</td>
<td>674803712 CentOS 7.3 (2).iso</td>
</tr>
<tr>
<td>a-----</td>
<td>6/12/2017 10:29 AM</td>
<td>674803712 CentOS 7.1 (3).iso</td>
</tr>
<tr>
<td>a-----</td>
<td>9/27/2017 3:03 AM</td>
<td>674803712 CentOS 7.0 (4).iso</td>
</tr>
<tr>
<td>a-----</td>
<td>10/3/2017 8:49 AM</td>
<td>2421367328 en_project_professional_2016_x64_dvd_6962336.iso</td>
</tr>
<tr>
<td>a-----</td>
<td>8/10/2017 10:55 AM</td>
<td>2421367328 en_project_professional_2016_64_dvd_6962336.iso</td>
</tr>
<tr>
<td>a-----</td>
<td>11/11/2017 11:45 AM</td>
<td>1469054976 Fedora-Live-Workstation-x86_64-23-10.iso</td>
</tr>
<tr>
<td>a-----</td>
<td>11/9/2017 2:31 PM</td>
<td>3020613776 Kali-Linux-2017.2-x86_64.iso</td>
</tr>
</tbody>
</table>
```

One-way hash example...

<table>
<thead>
<tr>
<th>Image Name</th>
<th>Download</th>
<th>Size</th>
<th>Version</th>
<th>sha256sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kali 64 bit</td>
<td>HTTP</td>
<td>2.8G</td>
<td>2017.2</td>
<td>4556775bf981ae64a3cb19aa0b73e8dcac6e4ba524f31c4bc14c9137b99725d</td>
</tr>
</tbody>
</table>

```powershell
PS C:\Users\tue87168> cd Downloads
PS C:\Users\tue87168\Downloads> dir *.iso

Directory: C:\Users\tue87168\Downloads

Mode  LastWriteTime     Length  Name
----  -------------  ------  -----
-a----  8/10/2017  10:55 AM  674803712  CSET 8.0 (1).iso
-a----  8/10/2017  11:03 AM  674803712  CSET 8.0 (2).iso
-a----  8/12/2017  10:29 AM  674803712  CSET 8.0.iso
-a----  8/12/2017  10:29 AM  674803712  CSET 8.0.0.iso
-a----  9/27/2017   3:00 PM  2421987328  en_project_professional_2016_x86_x64_dvd_6962236.iso
-a----  10/3/2017   8:49 PM  2421987328  en_visio_professional_2016_x86_x64_dvd_6962139.iso
-a----  11/11/2016  11:45 AM  1469054978  Fedora-Live-Workstation-x86_64-23-10.iso
-a----  11/9/2017   2:31 PM  3020619776  kali-linux-2017.2-amd64.iso

PS C:\Users\tue87168\Downloads> Get-FileHash kali-linux-2017.2-amd64.iso | Format-List

Algorithm : SHA256
Hash : 4556775bf981ae64a3cb19aa0b73e8dcac6e4ba524f31c4bc14c9137b99725d
Path : C:\Users\tue87168\Downloads\kali-linux-2017.2-amd64.iso
```
One-way hash example...

Notice the amount of **confusion** and **diffusion** resulting from a 1 character change!
Digital Signature

- A hash value encrypted with the sender’s private key
- The act of signing means encrypting the message’s hash value with the private key
**Strong cryptographic algorithms**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Algorithm Method</th>
<th>Key Size</th>
<th>Strength</th>
<th>Replaced By</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>Symmetric</td>
<td>64-bit block cipher</td>
<td>64 bit (56 + 8 parity)</td>
<td>Very weak</td>
<td>3DES</td>
</tr>
<tr>
<td>3DES</td>
<td>Symmetric</td>
<td>64-bit block cipher</td>
<td>192 bit (168 bit + 24 parity)</td>
<td>Moderate</td>
<td>AES</td>
</tr>
<tr>
<td>Blowfish</td>
<td>Symmetric</td>
<td>64-bit block cipher</td>
<td>32- to 448-bit key</td>
<td>Strong</td>
<td>N/A</td>
</tr>
<tr>
<td>AES</td>
<td>Symmetric</td>
<td>128-bit block cipher</td>
<td>128-bit encryption keys</td>
<td>Strong</td>
<td>N/A</td>
</tr>
<tr>
<td>Twofish</td>
<td>Symmetric</td>
<td>128-bit block cipher</td>
<td>128-, 192-, or 256-bit key</td>
<td>Strong</td>
<td>N/A</td>
</tr>
<tr>
<td>RC4 – Rivest Cipher 4</td>
<td>Symmetric</td>
<td>Stream mode cipher (one bit at a time)</td>
<td>40- to 2,048-bit key</td>
<td>Very Strong</td>
<td>N/A</td>
</tr>
<tr>
<td>RC5</td>
<td>Symmetric</td>
<td>Block mode cipher</td>
<td>Variable (up to 2048)</td>
<td>Very Strong</td>
<td>N/A</td>
</tr>
<tr>
<td>RSA</td>
<td>Asymmetric</td>
<td>Key transport</td>
<td>1024-bit keys</td>
<td>Strong</td>
<td>N/A</td>
</tr>
<tr>
<td>Diffie-Hellman</td>
<td>Asymmetric</td>
<td>Key exchange</td>
<td>N/A</td>
<td>Moderate</td>
<td>El Gamal</td>
</tr>
<tr>
<td>El Gamal</td>
<td>Asymmetric</td>
<td>Key exchange</td>
<td>N/A</td>
<td>Very Strong</td>
<td>N/A</td>
</tr>
<tr>
<td>MD5</td>
<td>Hashing - Integrity</td>
<td>Rivest MD5 Block Hash</td>
<td>512-bit block processing Creates 128-bit hashes / digest</td>
<td>Very weak</td>
<td>MD6, et. Al.</td>
</tr>
<tr>
<td>SHA-1</td>
<td>Hashing – Integrity</td>
<td>Rivest SHA Hash</td>
<td>512-bit processing Creates 160-bit hashes / digest</td>
<td>Weak</td>
<td>N/A</td>
</tr>
<tr>
<td>SHA-3</td>
<td>Hashing – Integrity</td>
<td>Hash</td>
<td>Creates 224-, 256-, 384-, or 512-bit hashes</td>
<td>Very Strong</td>
<td></td>
</tr>
</tbody>
</table>
# Reasons to Use Cryptography

<table>
<thead>
<tr>
<th>Reason</th>
<th>How achieved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>The message can be encrypted</td>
</tr>
<tr>
<td>Integrity</td>
<td>The message can be hashed and/or digitally signed</td>
</tr>
<tr>
<td>Authentication</td>
<td>The message can be digitally signed</td>
</tr>
<tr>
<td>Nonrepudiation</td>
<td>The message can be digitally signed</td>
</tr>
</tbody>
</table>
PKI Components

Digital Certificates
  • Contains Public Key identity and verification info

Certificate Authorities (CA)
  • Trusted entity that issues certificates

Registration Authorities (RA)
  • Verifies identity for certificate requests

Certificate Revocation List (CRL)
  • A list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted
Examples of Cryptanalysis Attacks

• Brute force
  • Trying all key values in the keyspace

• Frequency Analysis
  • Guess values based on linguistic analysis of frequency of occurrence of letters

• Dictionary Attack
  • Find plaintext based on common words

• Replay Attack
  • Repeating previous known values

• Known Plaintext
  • Format or content of plaintext available

• Man-in-the-Middle attack
  • Hacker intercepts traffic grabs two others’ public keys and replaces them with his/her own public key and uses his/her own private key to decrypt and monitors the traffic between the others
Quiz

1. The review of router access control lists should be conducted during:
   a. An environmental review
   b. A network security review
   c. A business continuity review
   d. A data integrity review

1. The review of router access control lists should be conducted during:
   a. An environmental review
   b. A network security review
   c. A business continuity review
   d. A data integrity review
Quiz

2. During an audit of a telecommunication system, an IS auditor finds that the risk of intercepting data transmitted to and from remote sites is very high. The MOST effective control for reducing this exposure is:
   a. Encryption
   b. Callback modems
   c. Message authentication
   d. Dedicated Leased lines

2. During an audit of a telecommunication system, an IS auditor finds that the risk of intercepting data transmitted to and from remote sites is very high. The MOST effective control for reducing this exposure is:
   a. Encryption
   b. Callback modems
   c. Message authentication
   d. Dedicated Leased lines
Quiz

3. A digital signature contains a message digest to:
   a. Show if the message has been altered after transmission
   b. Define the encryption algorithm
   c. Confirm the identity of the originator
   d. Enable message transmission in a digital format

3. A digital signature contains a message digest to:
   a. Show if the message has been altered after transmission
   b. Define the encryption algorithm
   c. Confirm the identity of the originator
   d. Enable message transmission in a digital format
Quiz

4. Digital signatures require the:
   a. Signer to have a public key and the receiver to have a private key
   b. Signer to have a private key and the receiver to have a public key
   c. Signer and receiver to have a public key
   d. Signer and receiver to have a private key
Quiz

5. When using public key encryption to ensure confidentiality of data being transmitted across a network:
   a. Both the key used to encrypt and decrypt the data are public
   b. The key used to encrypt is private, but the key used to decrypt the data is public
   c. The key used to encrypt is public, but the key used to decrypt the data is private
   d. Both the key used to encrypt and decrypt the data are private

5. When using public key encryption to ensure confidentiality of data being transmitted across a network:
   a. Both the key used to encrypt and decrypt the data are public
   b. The key used to encrypt is private, but the key used to decrypt the data is public
   c. **The key used to encrypt is public, but the key used to decrypt the data is private**
   d. Both the key used to encrypt and decrypt the data are private
6. During an audit of an enterprise that is dedicated to e-commerce, the IS manager states that digital signatures are used when receiving communications from customers. To substantiate this, an IS auditor must prove that which of the following is used?
   a. A biometric, digitized and encrypted parameter with the customer’s public key
   b. A hash of the data that is transmitted and encrypted with the customer’s private key
   c. A hash of the data that is transmitted and encrypted with the customer’s public key
   d. The customer’s scanned signature encrypted with the customer’s public key

6. During an audit of an enterprise that is dedicated to e-commerce, the IS manager states that digital signatures are used when receiving communications from customers. To substantiate this, an IS auditor must prove that which of the following is used?
   a. A biometric, digitized and encrypted parameter with the customer’s public key
   b. A hash of the data that is transmitted and encrypted with the customer’s private key
   c. A hash of the data that is transmitted and encrypted with the customer’s public key
   d. The customer’s scanned signature encrypted with the customer’s public key
Quiz

7. Email message authenticity and confidentiality is BEST achieved by signing the message using the:
   a. Sender’s private key and encrypting the message using the receiver’s public key
   b. Sender’s public key and encrypting the message using the receiver’s private key
   c. Receiver’s private key and encrypting the message using the sender’s public key
   d. Receiver’s public key and encrypting the message using the sender’s private key
Quiz

8. Which of the following effectively verify the originator of a transaction?
   a. Using a secret password between the originator and the receiver
   b. Encrypting the transaction with the receiver’s public key
   c. Using a portable document format (PDF) to encapsulate transaction content
   d. Digitally signing the transaction with the source’s private key
Quiz

9. Which of the following is the MOST effective type of antivirus software to detect an infected application?
   a. Scanners
   b. Active monitors
   c. Hash-based integrity checkers
   d. Vaccines
Agenda

✓ Team Presentation Schedule
✓ Cryptography and Cryptanalysis
✓ Terminology
✓ Symmetric Cryptography
✓ Asymmetric Cryptography
✓ Hashing and Digital Signature
✓ Public Key Infrastructure
✓ Cryptanalysis Attacks
✓ Quiz
Protecting Information Assets
- Unit# 11 -

Cryptography, Public Key Encryption and Digital Signatures