EE 491: Biometrics

Basic Concepts in Information Assurance

Definition

Information assurance:

- Information operations (IO) that protect and defend information and information systems (IS) by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.
- This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [INFOSEC -99]

Information Assurance

- Introduction
- Authentication and Identification
- Principles of Cryptography
- Modern Cryptography

Dependable systems

- Historical concerns.
- Perform operations CORRECTLY.
- Make computers AVAILABLE on regular basis.
- For some applications, system SAFETY become a major concern.
- SECURITY flaws may lead to catastrophic consequences too.
Information Assurance Module

Glossary

- **Availability**: readiness for usage.
- **Reliability**: Continuity of providing correct service.
- **Safety**: Non-occurrence of catastrophic failures.
- **Confidentiality**: Absence of non-authorized disclosure of information.

Glossary (2)

- **Integrity**: absence of improper alterations of information.
- **Non-repudiation**: creation of non-disputable evidence.
- **About the occurrence of a transaction.**
- **Authentication**: the process by which a claimed identity is verified.
- **Maintainability**: system's ability to undergo repairs and changes.

Glossary (3)

- **Protection**: measures that prevent the assets from being damaged.
- **Detection**: measures that allow for the detection of the extent, means and causes of damage.
- **Reaction**: measures that allow for the recovery of damaged assets.

Computer Security Breaches

- **Exposure**: unauthorized disclosure.
- **Vulnerabilities**: weakness of protection that might be exploited.
- **Attacks exploit vulnerabilities.**
- **Threats**: circumstances that make attacks likely to occur, vulnerabilities exposed.
- **Controls are the preventive measures countering the threats.**
Threats

- Interruption: loss of availability of an asset.
- Interception: gaining unauthorized access to an asset.
- Modification: tampering achieved through an interception.
- Fabrication: counter fitting, inserting transactions and/or records.

Threats to Computer Systems

- Fabrication
- Modification
- Interruption (Loss)
- Interception

Threats to Software

- Destruction
  - Configuration management essential
- Modification, alteration
  - SW performs more than required, or functionality progressively lost (time bomb)
- Subtle changes: Trojan horses, viruses, worms, trapdoors, information leaks
- Deletion, misplacement.

Other Exposed Assets

- Storage media
- Communication channels, networks
- Key people
  - Job security is an IA threat
  - White collar crime
  - Amateurs, crackers, career criminals, electronic warfare...

(A single point of attack)
The Real Threat

Percentage of Economic Loss attributed to Information Security Breach Categories. (Computer System Security and Privacy Advisory Board, National Institute of Standards and Technology (NIST), March, 1992)

- Internal Error 65%
- Unauthorized Employees 12%
- Malicious Outsiders 3%
- Infrastructure loss, water damage, etc. 13%
- Human Error 65%
- Dishonest Employees 13%
- Disgruntled Employees 6%
- Malicious outsiders 3%

Percentage of Economic loss attributed to information security breach categories. (Computer System Security and Privacy Advisory Board, National Institute of Standards and Technology (NIST), March, 1992)

<table>
<thead>
<tr>
<th>Types of Human Error</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Errors</td>
<td>20%</td>
</tr>
<tr>
<td>Password Issues</td>
<td>15%</td>
</tr>
<tr>
<td>Incorrect Accesses</td>
<td>10%</td>
</tr>
<tr>
<td>Input Errors</td>
<td>5%</td>
</tr>
<tr>
<td>Not following procedures</td>
<td>7%</td>
</tr>
<tr>
<td>Insecure Program</td>
<td>6%</td>
</tr>
<tr>
<td>Workload Issues</td>
<td>4%</td>
</tr>
<tr>
<td>Ignorance</td>
<td>1%</td>
</tr>
<tr>
<td>Failure to upgrade</td>
<td>1%</td>
</tr>
</tbody>
</table>

Key Factors Contributing to Human Error

- No/Adequate Training: 20%
- Not understanding Importance: 15%
- Time Pressure: 10%
- Irresponsibility: 10%
- Talking about issues outside: 5%
- No accountability: 5%
- No checks/balances: 5%
- Efforts to bypass security policy: 3%
- Inadequate resources: 2%

<table>
<thead>
<tr>
<th>Types of Human Error</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Efforts to bypass security policy</td>
<td>3%</td>
</tr>
<tr>
<td>No checks/balances</td>
<td>5%</td>
</tr>
<tr>
<td>Inadequate resources</td>
<td>2%</td>
</tr>
<tr>
<td>No accountability</td>
<td>5%</td>
</tr>
<tr>
<td>Talking about issues outside</td>
<td>5%</td>
</tr>
<tr>
<td>Time Pressure</td>
<td>10%</td>
</tr>
<tr>
<td>Not understanding Importance</td>
<td>15%</td>
</tr>
<tr>
<td>No/Adequate Training</td>
<td>20%</td>
</tr>
</tbody>
</table>

Information Assurance

- Introduction
- Authentication and Identification
- Principles of Cryptography
- Modern Cryptography
- Secure Information Exchange
User Identification
- The identity is a parameter in access control decisions.
- Identity is recorded in security-relevant event logs and audit trails.
- Most logins based on user name (identification) and password (authentication).
- Verification of the claimed identity.

Choosing Passwords
- Must keep the probability of an accidental guess low
- Guessing strategies:
  - Exhaustive search (brute force)
  - Intelligent search
    - Restricted search, names of friends and relatives, cars, registration number plates, phone numbers
    - Dictionary attacks

Authentication Procedures
- Begin the session with name/password pair
  - Repeated authentication leads to TOCTOU (time of check to time of use) problem
  - The first line of defense
  - Password related security threats
    - Password guessing
    - Password spoofing
    - Compromise of the password file

Defenses
- Set a password.
- Change default passwords.
- Password length.
- Password format.
- Avoid obvious passwords.
Let’s Talk Passwords

- A password needs to be at least 8 characters long (otherwise - can be machine guessed).
- Should be alphanumeric to help foil guessing.
- Changed regularly.
- Protected (many attacks are successful by obtaining password from the user).

Typical Password Usage

- A study in 1979 (Morris/Thompson)
  - 15 (.5%) were a single character
  - 72 (2%) were two ASCII characters
  - 464 (14%) were three ASCII characters
  - 477 (14%) were four alphabetic letters
  - 706 (21%) were five alphabetic letters
  - 605 (18%) were 6 alphabetic letters
  - 492 (15%) words in dictionaries or names
- Total studied = 3289; Total above = 2831 (86%)

A Moment on Passwords

- Typical Attacks -
  - Try all possible passwords
  - Try many probable passwords
  - Try passwords likely for user
  - Search for the System list of Passwords
  - Obtain from user

More Recent Studies

- 1990 (Klein): Repeated the experiment with about 14K passwords
  - 2.7% guessed in 15 minutes of machine time;
    21% within a week.
- 1992 (Spafford): Again - about 15K passwords:
  - Average password length 6.8 characters and 29% only lowercase alphabetic letters.
- 1997 (MSU): Cracker routine discovered >10% of passwords within one week.
Administrative Procedures
- Password checkers.
  - Perform regular ‘friendly’ dictionary attacks.
- Automated password generation.
- Password ageing.
- Limit login attempts.
- Informed user.
  - Display time of last login, # failed attempts since, recent attempted attacks.

Spoofing Attacks
- Spoofing attacks are the attempts to deceive or hoax computer authentication mechanisms.
- Username and password provide unilateral authentication.
  - How to check the identity of the verifier?
  - Fake login screens and password collection are the most common spoofs.

Does This Work?
- Difficulty memorizing passwords.
  - Found written underneath the keyboard.
- Difficult to comply with password admin.
- Forgotten password disrupts user’s work.
  - Is the request for a new password coming from a legitimate user?
- Successful attacks are based on social engineering, rather than technical skills.

Spoofing Attacks (2)
- Countermeasures:
  - Display the number of failed logins.
  - Trusted path (ALT+CTRL+DEL for WinNT).
  - Mutual authentication.
    - Typically, user identifies itself to the system he/she needs to access.
    - Mutual identification requires that the system identifies itself to the user too. This requires 2-way authentication schemes.
Beyond Spoofing

- In reality, passwords are stored in a number of 'intermediate' locations.
  - Buffers, cache memory, network, web servers...
- On-line banking problem:
  - Using the BACK button on a browser can lead back into a restricted area.
  - User MUST terminate the browser execution.
  - Users asked to participate in memory management activity!

Protecting Password Files

- Password salting:
  - When storing the encrypted password, append something to it.
  - Same passwords will have 'different' encryptions.
  - Slows down dictionary attacks.
- Lessons learned:
  - Combination of mechanisms can enhance protection.
  - Security by obscurity protects against casual intruders only.
  - Separate security relevant data from the rest.

Protecting Password Files

- Cryptographic protection.
  - One way encryption algorithms.
  - This doesn't prevent dictionary attacks.
  - Proper choice of encryption may slow down dictionary attacks – UNIX crypt(3).
- Access control enforced by the OS.
  - New versions of UNIX store passwords in so called shadow password files (separate from /etc/passwd).
  - NT stores encrypted passwords in proprietary binary formatted file (security by obscurity).

Single Sign-on

- Resource based passwords awkward.
  - Workstation, network, server, database management system, a table in a database all have separate passwords.
- Rather, single sign-on automatically relates the passwords.
  - More convenient, but presents design problems and potentially creates additional vulnerabilities.
Alternative Approaches

- Something you know.
  - Pass-codes, pins, DOB, maiden name...
  - The user cannot prove innocence in case of a misuse.
- Something you hold.
  - Physical tokens, like keys, magnetic cards, identity tags, smart cards.
- Who you are.
  - Biometrics: face, fingerprint, voice, hand geometry, retina scans, iris scans...
  - Handling of false positives and false negatives.

Summary

- A password DOES NOT authenticate a person!
  - Authentication implies a user knew the password.
- This is an inherent limitation, an issue where biometric devices provide advantage.
- Biometric authentication shares other concerns of computer authentication.
  - Admin procedures, spoofing attacks, memory protection, authentication file protection, single sign-on procedures.
- Coherent approach to design and verification/validation of biometrics based authentication services is needed.

Alternative Approaches (Cont.)

- What you do.
  - Other kinds of biometrics: written signatures, typing patterns, etc.
  - Need to be fine tuned for specific applications.
- Where you are.
  - Allow system login only from certain terminals.
  - Suitable for mobile and distributed computing.
  - GPS based authentication may resolve disputes about user’s identity (in case of a misuse).

Information Assurance

- Introduction
- Authentication and Identification
- Principles of Cryptography
- Modern Cryptography
- Secure Information Exchange
Encryption Basics
- Disguising a message content.
- Maintaining secure data in an insecure environment.
- Weakest link principle.
- Study of the principles of encryption.
- Study of how encryption fails.

Terminology and Background
- Encryption is a process of encoding a message so that its meaning is not obvious.
- Decryption is the reverse process.
- A system for encryption and decryption is called a cryptosystem.

Cryptosystems
- Keyless cipher
  - Plaintext $P = (p_1, p_2, ..., p_n)$.
  - Ciphertext $C = (c_1, c_2, ..., c_n)$.
  - $C = E(P)$, $P = D(C)$.
  - $P = D(E(P))$.

Cryptosystems (2)
- Symmetric cryptosystem.
  - Plaintext $P = (p_1, p_2, ..., p_n)$.
  - Ciphertext $C = (c_1, c_2, ..., c_n)$.
  - $C = E(K, P)$, $P = D(K, C)$.
  - $P = D(K, E(K, P))$.
- $E$ and $D$ are mirror processes.
Cryptosystems (3)

Asymmetric cryptosystem.
- Plaintext $P=(p_1, p_2, ..., p_n)$.
- Ciphertext $C=(c_1, c_2, ..., c_n)$.
- $C=E(K_E, P), \ P=D(K_D, C)$.
- $P=D(K_D, E(K_E, P))$.
- Different encryptions of the same message possible by changing key pairs.

Breakable Encryption

- Having enough time and data, any encryption is breakable.
- Practicality:
  - Assume $10^{30}$ decipherments. Computer able to guess $10^{10}/s$.
  - Need $10^{20}$ seconds ~ $10^{12}$ years.
  - But this assumes a brute force approach!
- Is $10^{30}$ system breakable?
  - Yes, eventually!

Cryptanalysis

- Attempt to break a single message.
- Recognize patterns in encrypted messages and approximate a decryption algorithm.
- Find weaknesses in encryption algorithms.
- A cryptanalyst's Resources:
  - Encrypted messages, known algorithms, intercepted plaintext, suspected message content, mathematical/statistical tools and techniques, properties of languages, computers, ingenuity and luck...

Breakable Encryption (2)

- Is $10^{30}$ system breakable?
  - Assume that $10^{30}$ options are somehow (intelligent search) reduced to $10^{15}$.
  - With $10^{10}$ ciphers checked per second, it takes less than 30 hours to break the system.
- Technological advances make infeasible computations feasible within a decade.
- Breakability defined by current technology.
Cryptography: Simple Methods

- **Monoalphabetic ciphers**
  - Substitutions (letter exchanges)
  - Transpositions (rearranging the order of letters)

- **Polyalphabetic ciphers**

- **Character representations**
  - English alphabet: A-Z
  - Letters: A B C D E Y Z
  - Numbers: 0 1 2 3 4 24 25
  - A + 3 = D, K - 1 = J, etc.
  - Plaintext: upper case, Ciphertext: lowercase

Substitutions

- **Caesar cipher**
  - \( c_i = E(p_i) = p_i + 3 \)
  - Example: B I O M E T R I C S
    e l r p h w u l f v
  - Advantages: Easy to perform in the field, easy to remember
  - Disadvantage: Obvious pattern.

Cryptanalysis of Monoalphabetic Ciphers

- **Clues:**
  - Short words, repeated letters, common initial and final word letters.
  - Guess and substitute until you reach a solution or a contradiction.
  - Letter frequency distributions.
    - Language dependent.
    - Field (of the message) dependent.
    - Age dependent.

Caesar Cipher: Cryptanalysis

- \( w k l v \ p h v v d j h \ l v \ q r w \ w r r \ k d u g \ w r \ e u h d n \)

- Too many obvious clues.
  - Short English words, word breaks, blank-to-blank mapping (frequently masked).
  - Any permutation is a legal cipher
    - \( ? \left( ? \right) = 25 \) \( ? \left( ? \right) = 3 \cdot ? \mod 26 \).
  - Keywords (for example, SPECTACULAR)
    - A B C D E Y Z
    - 0 1 2 3 4 24 25
### Polyalphabetic Ciphers

- **Goal**: Secure ciphertext should have a flat alphabet distribution.
- **Mean**: Combine different encoding schemes.

### Table 2-1: Letter Frequency Distributions in English and Pascal

<table>
<thead>
<tr>
<th>Letter</th>
<th>English Count</th>
<th>Percent</th>
<th>French Count</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>1312</td>
<td>4.30</td>
<td>464</td>
<td>4.30</td>
</tr>
<tr>
<td>b</td>
<td>773</td>
<td>1.29</td>
<td>357</td>
<td>3.12</td>
</tr>
<tr>
<td>c</td>
<td>199</td>
<td>0.34</td>
<td>93</td>
<td>0.81</td>
</tr>
<tr>
<td>d</td>
<td>2452</td>
<td>4.51</td>
<td>511</td>
<td>4.51</td>
</tr>
<tr>
<td>e</td>
<td>4192</td>
<td>14.00</td>
<td>1921</td>
<td>15.81</td>
</tr>
<tr>
<td>f</td>
<td>966</td>
<td>1.74</td>
<td>966</td>
<td>1.74</td>
</tr>
<tr>
<td>g</td>
<td>769</td>
<td>1.74</td>
<td>769</td>
<td>1.74</td>
</tr>
<tr>
<td>h</td>
<td>266</td>
<td>0.42</td>
<td>266</td>
<td>0.42</td>
</tr>
<tr>
<td>i</td>
<td>254</td>
<td>0.46</td>
<td>254</td>
<td>0.46</td>
</tr>
<tr>
<td>j</td>
<td>139</td>
<td>0.27</td>
<td>139</td>
<td>0.12</td>
</tr>
<tr>
<td>k</td>
<td>206</td>
<td>0.47</td>
<td>206</td>
<td>0.47</td>
</tr>
<tr>
<td>l</td>
<td>1079</td>
<td>2.27</td>
<td>1079</td>
<td>2.27</td>
</tr>
<tr>
<td>m</td>
<td>1500</td>
<td>3.29</td>
<td>1500</td>
<td>3.29</td>
</tr>
<tr>
<td>n</td>
<td>286</td>
<td>0.56</td>
<td>286</td>
<td>0.56</td>
</tr>
<tr>
<td>o</td>
<td>3263</td>
<td>7.37</td>
<td>855</td>
<td>7.55</td>
</tr>
<tr>
<td>p</td>
<td>1874</td>
<td>4.23</td>
<td>340</td>
<td>3.12</td>
</tr>
<tr>
<td>q</td>
<td>126</td>
<td>0.26</td>
<td>12</td>
<td>0.12</td>
</tr>
<tr>
<td>r</td>
<td>278</td>
<td>0.64</td>
<td>1147</td>
<td>10.12</td>
</tr>
<tr>
<td>s</td>
<td>610</td>
<td>1.31</td>
<td>594</td>
<td>1.31</td>
</tr>
<tr>
<td>t</td>
<td>858</td>
<td>1.95</td>
<td>1031</td>
<td>9.28</td>
</tr>
<tr>
<td>u</td>
<td>1529</td>
<td>3.33</td>
<td>277</td>
<td>2.56</td>
</tr>
<tr>
<td>v</td>
<td>512</td>
<td>1.16</td>
<td>178</td>
<td>1.60</td>
</tr>
<tr>
<td>w</td>
<td>125</td>
<td>0.28</td>
<td>139</td>
<td>0.12</td>
</tr>
<tr>
<td>x</td>
<td>327</td>
<td>0.69</td>
<td>303</td>
<td>2.77</td>
</tr>
<tr>
<td>y</td>
<td>12</td>
<td>0.04</td>
<td>15</td>
<td>0.12</td>
</tr>
<tr>
<td>z</td>
<td>16</td>
<td>0.04</td>
<td>5</td>
<td>0.05</td>
</tr>
<tr>
<td>All</td>
<td>4473</td>
<td>100.00</td>
<td>14153</td>
<td>100.00</td>
</tr>
</tbody>
</table>

### Breakability (Again)

- Short messages more difficult to break.
- Ideally: $26! \approx 4 \times 10^{26}$ different permutations.
  - Frequency counts significantly narrow the search.
- Cryptographer's dilemma:
  - Regular encryption algorithms are easy to remember and apply.
  - Regularity gives clues to cryptanalysis!
- Timeliness measure:
  - A security measure must be strong enough to keep out the attacker for the life of the data.
  - Short time value data protected with simple measures.

### Polyalphabetic Ciphers (2)

- Combination of 2 encryption alphabets.
  - Characters in odd positions:
    - $\text{odd}(?) = (3 \times ?) \mod 26$.
  - Characters in even positions:
    - $\text{even}(?) = (5 \times ????) \mod 26$.
Net Effect of Multiple Ciphers

From Dickens', "A tale of two cities", opening paragraph.

? 1(?) = ?, 2(?) = 25 - ?

Vigenere Tables

- Permutations should be complements.
- Extend the number of permutations.
- But how to keep track?

<table>
<thead>
<tr>
<th>Table 2-3 Vigenere Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
</tr>
<tr>
<td>0</td>
</tr>
</tbody>
</table>

Vigenere Tables: Example

- 1st column: plaintext letter.
- 1st row: key alphabet.
- Write alphabet keyword (bojan) above the plaintext, use it for selecting the permutation.

Table 2-4 Two-Alphabet Encryption Letter Frequencies

<table>
<thead>
<tr>
<th>Letter</th>
<th>Count</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>14</td>
<td>4.04</td>
</tr>
<tr>
<td>b</td>
<td>11</td>
<td>2.77</td>
</tr>
<tr>
<td>c</td>
<td>12</td>
<td>3.00</td>
</tr>
<tr>
<td>d</td>
<td>17</td>
<td>4.30</td>
</tr>
<tr>
<td>e</td>
<td>18</td>
<td>4.56</td>
</tr>
<tr>
<td>f</td>
<td>16</td>
<td>4.15</td>
</tr>
<tr>
<td>g</td>
<td>14</td>
<td>3.64</td>
</tr>
<tr>
<td>h</td>
<td>7</td>
<td>1.74</td>
</tr>
<tr>
<td>i</td>
<td>15</td>
<td>3.81</td>
</tr>
<tr>
<td>j</td>
<td>1</td>
<td>0.25</td>
</tr>
<tr>
<td>k</td>
<td>12</td>
<td>3.00</td>
</tr>
<tr>
<td>l</td>
<td>10</td>
<td>2.56</td>
</tr>
<tr>
<td>m</td>
<td>9</td>
<td>2.30</td>
</tr>
<tr>
<td>n</td>
<td>10</td>
<td>2.56</td>
</tr>
<tr>
<td>o</td>
<td>10</td>
<td>2.56</td>
</tr>
<tr>
<td>p</td>
<td>9</td>
<td>2.30</td>
</tr>
<tr>
<td>q</td>
<td>1</td>
<td>0.25</td>
</tr>
<tr>
<td>r</td>
<td>14</td>
<td>3.64</td>
</tr>
<tr>
<td>s</td>
<td>14</td>
<td>3.64</td>
</tr>
<tr>
<td>t</td>
<td>14</td>
<td>3.64</td>
</tr>
</tbody>
</table>

**Information Assurance**
- Introduction
- Authentication and Identification
- Principles of Cryptography
- Modern Cryptography
- Secure Information Exchange

---

**Public Key Encryption Systems**
- Proposed in late seventies.
- Requires pairs of keys
  - Public and private
  - Encryption and decryption.
- The same key pair can be used longer.
  - In secret key systems, a different key may be needed for each transmission.
- $P = D(K_{PRIVATE}, E(K_{PUBLIC}, P))$.
- $P = D(K_{PUBLIC}, E(K_{PRIVATE}, P))$.

---

**Asymmetric Cryptosystems**
- Plaintext $P = (p_1, p_2, ..., p_n)$.
- Ciphertext $C = (c_1, c_2, ..., c_n)$.
- $C = E(K_E, P)$, $P = D(K_D, C)$.
- $P = D(K_D, E(K_E, P))$.
- Different encryptions of the same message possible by changing key pairs.

---

**RSA (Rivest, Shamir, Adelman)**
- Developed in 1978 by MIT scientists.
- Remains “secure” up to date.
  - No proof, just a high confidence level.
- Encryption:
  - $C = P^e \mod n$
- Decryption:
  - $P = C^d \mod n$
  - Algorithm based on factoring of large numbers, the problem is computationally exponential.
RSA (2)

- \( P = C^d \mod n = (P^e)^d \mod n \)
- \( d \) and \( e \) are INVERSES.

Choosing keys:
- Encryption key \((e,n)\)
- Decryption key \((d,n)\)
- Typically \((e,n)\) is a public key, \((d,n)\) is a private key.

1. \( n \) LARGE, a product of 2 primes, \( p \) & \( q \).
   - Large \( n \) prevents factoring.
2. Choose \( e \), relative prime to \((p-1)*(q-1)\)
3. Select \( d \), s.t. \( e*d=1 \mod (p-1)*(q-1) \)

RSA Example

- \( p=47, \ q=71 \). Then \( n=p*q=3337 \).
- \( (p-1)*(q-1)=46*70=3220 \).
- Choose \( e \), a relative prime to 3220.
  - \( e=79 \).
- Select \( d \), \( e*d=1 \mod 3220 \).
  - \( d=1019, \ e*d=79*1019=80501; \ 80501 \mod 3220=1 \).
- Encryption, \( P=668 \).
  - \( C=668^{79} \mod 3337 = 1570 \).
- Decryption:
  - \( P = C^{1019} \mod 3337 = 1570^{1019} \mod 3337 = 668 \).

RSA Implementation

- Choose 2 primes, \( p \) and \( q \).
  - \( p \) and \( q \) \( \sim 100 \) decimal digits each.
  - Compute \( n=p*q, \ n \sim 200 \) digits (\( n \sim 512 \) bits).
- Choose \( e \) relative prime to \((p-1)*(q-1)\).
  - Usually, \( e \) is larger than each factor.
- Compute \( d \) as an inverse of \( e \).
- USER:
  - Distributes \( e \) and \( n \).
  - Keeps secret \( d \).
  - Discard (without revealing): \( p, \ q, \ (p-1)*(q-1) \).

Symmetric Encryption

- Advantage: symmetry, speed.
- Difficulties:
  - Stolen keys.
  - Key distribution (multiple independent channels).
  - A separate key for each sender/receiver pair.
  - Generally, weaker encryption.
Data Encryption Standard (DES)

- Developed for the US government (70’s).
- An officially accepted standard.
  - Uses simple logical operations on ‘small’ numbers.
- Combines substitutions and transpositions.
  - Repeated application, 16 times.
  - Variable key length.
  - Implemented in software or single-purpose chips.
  - Operates on 64-bit long blocks of data.

Inside DES

This operation are repeated 16 consecutive times.

Same function, applied backwards, decrypts the message.

DES Security

- Depends on the key length.
  - On Tuesday, January 19, 1999, distributed.net, a worldwide coalition of computer enthusiasts, worked with EFF’s DES cracker and a worldwide network of nearly 100,000 PCs on the internet, to win RSA data security’s DES challenge III in a record-breaking 22 hours and 15 minutes. The team deciphered a secret message encrypted with the data encryption standard (DES) algorithm using commonly available technology. From the floor of the RSA data security conference & expo, a major data security and cryptography conference being held in San Jose, Calif., EFF’s DES cracker and the distributed.net computers were testing 245 billion keys per second when the key was found.
  - This is a cheap solution, demonstrating how security estimates can be based on flawed assumptions.

DES Security (2)

- DES does not have known significant weaknesses.
- But, DES has become an obvious target.
- Trend towards sealed encryption devices.