Encryption

COMP620 Information Privacy & Security

Historical Encoding

- People have been writing secret messages for millennia
- The Caesar cipher (shift cipher) is said to have been used by Julius Caesar
- Computational efficiency was very important before computers

Cryptography

- Cryptography in general represents the process of encrypting a plain-text file into an unreadable cipher so that it can be stored and decrypted by the intended recipient.
- Cryptography is an important tool for security.

Encryption Media

- Encryption can be used to secure information sent over a network.
- Encryption can also be used to secure data stored on a computer.

Key

Plaintext → Encryption → Decryption → Plaintext
Shift Cipher

- The letters of the alphabet are shifted by a fixed amount
- Key is the number of letters to shift
- Can easily be defeated by trying all 26 possible shifts

Decryption by Brute Force

- Frpsxwhuv duh ixq
- Eqorwvgtu ctg hwp
- Dpnqvufst bsf gvo
- Computers are fun

Substitution Cipher

- Letters are mapped to symbols or letters
- Key – An alphabetical list of the symbols

Letter Frequency

The frequency of the use of a letter in English

- There are 26! = 4x10^26 possible keys
Text Translated by Frequency

- welcome to north carolina
  agricultural and technical state
  university! as you explore our
  website, you will have the
  opportunity to discover a&t’s
  rich and storied history and
  learn about our award-winning
  faculty, intensive
  research programs, and
  student-led
  community service initiatives.

  Chancellor Martin

Original Text

- welcome to north carolina
  agricultural and technical state
  university! as you explore our
  website, you will have the
  opportunity to discover a&t’s
  rich and storied history and
  learn about our award-winning
  faculty, intensive
  research programs, and
  student-led
  community service initiatives.

  Chancellor Martin

Onetime Pad

- With onetime pad encryption, the bit stream
  of the message is XOR with a random key
- The key must be at least as long as the
  message so it is not repeated
- The key must be truly random, not just
  pseudo-random

Perfect Encryption

- Onetime pad is a perfect encryption technique
  that cannot be broken
- A given cipher text can be decrypted into any
  possible plain text by using the appropriate key

<table>
<thead>
<tr>
<th>Cipher Text</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>011001010</td>
<td>001100000</td>
</tr>
<tr>
<td>010101010</td>
<td>011010101</td>
</tr>
<tr>
<td>000011111</td>
<td>011010101</td>
</tr>
</tbody>
</table>
Diffusion and Confusion

- **Diffusion** – spread the plain text data across the cipher text. A byte of plain text should impact many bytes of cipher text.
- **Confusion** – change the bits of the plain text according to some rule.

Types of Encryption

- **Symmetric Key or Secret Key**
  - The encryption key is the same as the decryption key.
  - Sender and receiver have to securely share a key.
- **Asymmetric Key or Public Key**
  - The key to decrypt is different, but related to, the key to encrypt.
  - The encryption key can be made public while the decryption key is kept secret.

Symmetric Key Cryptography

- Keys exchanged prior to communications. Parties verified at that time.
- Key to encrypt message is the same as key to decrypt.
- DES and AES are examples of Symmetric Key Cryptography.

Why Publish a Standard?

- The Data Encryption Standard (DES) and Advanced Encryption Standard (AES) algorithms are published and well known.
- Why not keep the algorithm secret?
- To be useful, others have to implement it.
- A good encryption algorithm will allow only those with a key to access the data. Knowing the algorithm does not give you access.
Asymmetric Key Cryptography

- Public key different from private key.
- RSA encryption is an example of Asymmetric Key Cryptography.

Encryption Performance

- RSA asymmetric key encryption is slower than DES or AES.
- DES and AES are easy to implement in hardware.
- AES can be efficiently implemented in software.
- Hybrid encryption uses both asymmetric and symmetric key systems.

Key Strength

- The longer they key, the harder it is to defeat the encryption by brute force.
- If the key is $n$ bits, it requires $2^n$ guesses to try all possible keys. You are likely to guess correctly in $2^{n-1}$ tries.
- Asymmetric key algorithms require a mathematical relation between the keys so not every bit string can be a key.

Key Lengths

- DES uses a 56 bit key
- Triple DES or DES3 uses two DES keys for a total of 112 bits
- AES uses 128, 192 or 256 bit keys.
- RSA uses variable length keys, frequently 512, 1024 or 2K bits in length.
Brute Force Decryption

- Brute force tries all possible keys.
- In 1998 the Electronic Frontier Foundation built a device that could brute-force a DES key in less than 2 days.

Hybrid Cryptography (STEP 1)

- DES key is encrypted with asymmetric key cryptography using Public Key of receiver.
- DES key sent to receiver.
- Both users end up with a shared DES key.

Hybrid Cryptography (STEP 2)

- Message is encrypted with the DES key previously sent to the receiver.
- DES key is discarded after sending the message.

Encryption Methods

- Block Cipher – one block of plaintext is encrypted to one block of ciphertext.
**Encryption Methods**

- Stream Cipher – blocks are XORed with previous blocks.

**Steganography**

- **Steganography** is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message.
- A form of security through obscurity

**Steganography in Images**

- Removing all but the last 2 bits of each color from the tree picture component produces an almost completely black image. Making that image 85 times brighter produces the cat image.

**Steganography and Encryption**

- You can use both steganography and encryption to send a hidden encoded message.
- A simple method is to encrypt the message and then hide it in the least significant bits of an image.
Coded Message

By counting the number of letters between those letters whose "tails" point upwards, we get the following sequence of numbers.

Donald does it was good news to hear that
3 3 5 1 5 1 4 1 2 3 4

you have found a job in Paris. Anna hopes
3 3 3 5 1 4 5 1 2 4

33 51 51 41 23 43 33 51 45 12 43 24 11 34 34 11 34 42 33 11 44 42 43 33

Now use the following table to decrypt this message:

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>F</th>
<th>L</th>
<th>Q</th>
<th>V</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>B</td>
<td>G</td>
<td>M</td>
<td>R</td>
<td>W</td>
</tr>
<tr>
<td>3</td>
<td>C</td>
<td>H</td>
<td>N</td>
<td>S</td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>D</td>
<td>I</td>
<td>J</td>
<td>O</td>
<td>T</td>
</tr>
<tr>
<td>5</td>
<td>E</td>
<td>K</td>
<td>P</td>
<td>U</td>
<td>Z</td>
</tr>
</tbody>
</table>

To get: NEEDMONEYFORASSASSINATION