Cryptography

CS 166: Introduction to Computer Systems Security
Security Goals?

Confidentiality

Availability

Integrity

CIA Triad
Standard Communication

Sender

communication channel

Recipient

sent message

received message
Eavesdropping

sent message

read

received message

Sender

Attacker

Recipient

Cryptography

2/1/16
Blocking

sent message

Recipient

received message

Sender

Attacker

drop

A@acker

drop

Cryptography
Cryptography

- Cryptography provides methods for assuring the confidentiality and integrity of data that is
  - transmitted over communication channels (e.g., web pages and email messages)
  - stored on devices (e.g., files on a laptop or data center)
- We focus on confidentiality protection for today.
Encrypted Communication

sender

encrypt

plaintext

ciphertext

decrypt

plaintext

Attacker

Recipient

2/1/16

Cryptography
Encryption

• Encryption allows to secure communications
  – Originally focused on confidentiality alone

• Encryption combines the plaintext with an encryption key to produce the ciphertext
  – The ciphertext is transmitted instead of the plaintext

• Decryption combines the ciphertext with the decryption key to return the plaintext
  – Only the intended recipient should have the secret key

• Encryption and decryption should be computationally infeasible without the corresponding keys
CLASSIC CRYPTOGRAPHY
Classic Encryption Methods

• Used for military applications since ancient times
• Julius Caesar’s cipher
  – replace a with x
  – replace b with y ...

• Alphabet shift cipher
  – Method: replace each character c of the plaintext with the character k positions after c in the alphabet
  – Key (for encryption and decryption): number k
  – Can be easily cracked by trying all possible values of k between 1 and the size of the alphabet
Substitution Cipher

- Arbitrary permutation of the characters
  - A ➔ K
  - B ➔ T
  - C ➔ G
  - ...
- The key is the sequence of permuted characters (KTG ...)
- Number of possible keys for 26-character alphabet ≈ $4 \times 10^{26}$
- Unfeasible to try all possible keys but ...
- Can be cracked by frequency analysis
  - Most frequent letters in English: e, t, o, a, n, i, ...
  - Most frequent digrams: th, in, er, re, an, ...
  - Most frequent trigrams: the, ing, and, ion, ...
- Attack first described in a 9th century book by al-Kindi
Frequency Analysis (1)

Example

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: “DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPD. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?” OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

2/1/16 Cryptography 13
Frequency Analysis (2)

PCQ VMJYPD THYK TYSE KHXHJWXV HXV ZCJPE EYPD KHXHYUXJ THJEE KCPK. CP THE THCMKXPV XPV IYJKT PYDHT, QHEP KHO HXV EPVEV THE LXRE CI SX'XJMI, KHE JCKE XPV EYKKEV THE DJCMPV ZEICJE HYS, KXUYPD: “DJEXT EYPD, ICJ X THCMKXPV XPV CPE PYDHTK Y HXNE ZEEP JEACMPTYPD TC UCM THE IXZREK CI FXKT XDEK XPV THE REDEPVK CI XPAYEPT EYPDK. SXU Y SXEE KC ZCRV XK TC AJXNE X IXNCMJ CI UCMJ SXGEKTU?”

EFYRCDME, TXREK IJCS THE THCMKXPV XPV CPE PYDBTK

More guesses

• J → ...

... R

2/1/16

Cryptography
Frequency Analysis (2)

PCQ VMRYPD THYK TYSE KHXHRXWXV HXV ZCRPE EYPD KHXHYUXR THREE KCPK. CP THE THCMKXPV XPV IYRKT PYDHT, QHEP KHO HXV EPVEV THE LXRE CI SX’XRMI, KHE RCKE XPV EYKKEV THE DRCMPV ZEICRE HYS, KXUYPD: “DREXT EYPD, ICR X THCMKXPV XPV CPE PYDHTK Y HXNE ZEEP REACMPTYPD TC UCM THE IXZREK CI FXKT XDEK XPV THE REDEPVK CI XPAREPT EYPDK. SXU Y SXEE KC ZCRV XK TC ARXNE X IXNCMJ CI UCMRSXGEKITU?”

More guesses

- J ➔ ...
- R
- K ➔ ...
- S
- X ➔ ...
- A

2/1/16 Cryptography
Letter Frequencies Graph

Common Digrams
- In English: th, he, in, er, an
- In MESSAGE: LB, PV, BO, XP, CM

Common Trigrams
- In English: the, and, tha, ent, ing
- In MESSAGE: XPV, YPD, LBO, EYP, LBC
Now during this time Shahrazad had borne king Shahriyar three sons. On the thousand and first night, when she had ended the tale of Ma’aruf, she rose and kissed the ground before him, saying: “great king, for a thousand and one nights I have been recounting to you the fables of past ages and the legends of ancient kings. May I make so bold as to crave a favour of your majesty?”

Epilogue, Tales from the Thousand and One Nights

To experiment with classic cryptography, visit www.cryptoclub.org
Requirements of Modern Cryptography

• Kerckhoff’s Principle (1883)

security based on key only, adversary knows cryptographic method

aka “no security by obscurity”
Symmetric Key Cryptography

- Same key used for encryption and decryption
- Encryption and decryption algorithms are one the reverse of the other
Symmetric Key Cryptography

• Advantages
  – Conceptual simplicity
  – Suitable for one-to-one communication (e.g. confidential email)

• Disadvantages
  – Setup requires secure channel to exchange key
  – Unsuitable for many-to-many communication (e.g. sharing secure data)
Modern Symmetric Cryptography

Data Encryption Standard (DES)
- Developed by IBM in collaboration with the NSA
- Became US government standard in 1977
- 56-bit keys
- Exhaustive search attack feasible since late 90s

Advanced Encryption Standard (AES)
- Selected as US government standard in 2001 through open competition
- 128-, 192-, or 256-bit keys
- Exhaustive search attack not currently possible
One-Time Pads
# Bitwise XOR

<table>
<thead>
<tr>
<th>bit 1</th>
<th>bit 2</th>
<th>resulting bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
One-Time Pad

- **Key**
  - Sequence of random bits
  - Same length as plaintext

- **Encryption**
  - $P =$ plaintext; $K =$ key
  - $C = K \oplus P$ (bit-wise XOR)
  - Example
    - $P = 01101001$
    - $K = 10110010$
    - $C = 11011011$

- **Decryption**
  - $P = K \oplus C$ (bit-wise XOR)

- **Advantages**
  - Each bit of the ciphertext is random
  - Fully secure if key used only once

- **Disadvantages**
  - Key as large as plaintext
    - Difficult to generate and share
  - Key cannot be reused
Pitfalls with One-Time Pads

- Key reuse

Source: Cryptosmith and David Lowry-Duda, Cryptography Stack Exchange
Pitfalls with One-Time Pads

• Imperfectly distributed pixels

Source: Justin Bisignano and Joshua Liebow-Feeser
See http://cs.brown.edu/courses/cs166/demos/
Pitfalls with One-Time Pads

• Imperfect randomness

Source: Justin Bisignano and Joshua Liebow-Feeser
See http://cs.brown.edu/courses/cs166/demos/
Security coordinate  
1. Confidentiality  
2. Integrity  
3. Availability

A general attack  
1. Eavesdropping  
2. Tampering  
3. Blocking

Crypto Intro

- Encryption and Decryption
- Symmetric systems use the same key
- One Time Pad