NOVEMBER 3 – 4

TexSAW 2017

7th ANNUAL
TEXAS SECURITY AWARENESS WEEK

ERIK JONSSON SCHOOL OF ENGINEERING & COMPUTER SCIENCE

THE UNIVERSITY OF TEXAS AT DALLAS

UT DALLAS

State Farm®
Cryptography
● Introduction
● Classical Confidentiality
● Modern Confidentiality
● Integrity
● Authentication
Introduction
Cryptography in the Real World

- Cryptography is the process of writing or reading secret messages or codes (Merriam Webster)
- Been used throughout recorded history
Terminology

- **Plaintext**
  - The original readable message

- **Ciphertext**
  - An encrypted message

- **Cipher**
  - An algorithm to convert plaintext to ciphertext and vice versa

- **Key**
  - A string that modifies the cipher
Uses for Cryptography

- Confidentiality
  - Used since the dawn of recorded history to protect information
  - Continues to this day aided by computers
- Integrity
  - Provides some information that can be used to determine if a message has been changed
- Authentication
  - Allows proof that you are who you say you are
Classical Cryptography
Early Classical Cipher Categories

- Classical ciphers worked with the symbols used in their language
- Substitution Cipher
  - Replace the symbols in the message with other symbols according to some key
- Transposition Cipher
  - Rearrange the symbols according to the key
Substitution Ciphers

- A mapping is created based on the key
- Symbols in the message are substituted based on the mapping
- Both sides need to know the mapping to encode or decode the message

Examples:
- Caesar Cipher
- Substitution Cipher
- Vigenère Cipher
Caesar Cipher

- Shift the alphabet a certain number of places
- The key is the number of places shifted
- How to defeat?

Caesar Cipher with a shift of 3

<table>
<thead>
<tr>
<th>Plain Text: Hello</th>
<th>Cipher Text:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABCDEFGHIJKLMNOPQR</td>
<td>wxyzabcdefg</td>
</tr>
</tbody>
</table>
Caesar Cipher - How To Defeat

- Only 26 permutations
  - 25 since one is to change nothing
- Try every combination
- Look for common patterns dependant upon language
- How could you improve?
Substitution Cipher

- Generate a mapping where each symbol is paired with another symbol independent of the others
- Key is the mapping string
- How many possible mappings?
- How to defeat?
Substitution Cipher - How To Defeat

- Number of occurrences of a symbol
  - A symbol is always mapped with another symbol
- Use frequency analysis to determine the most common symbols
  - Work from the most common
- How to improve?
Vigenère Cipher

• Artificially extend the key to be the length of the plaintext.
• Plaintext $P = p_0 p_1 p_2 \ldots p_{m-1}$
• Ciphertext $C = c_0 c_1 c_2 \ldots c_{m-1}$
• Key $K = k_0 k_1 \ldots k_{n-1}$
• Encryption: $C_i = (P_i + k_{i \mod n}) \mod 26$
• Decryption: $P_i = (C_i - k_{i \mod n}) \mod 26$
Vigenère Cipher

• To encrypt:
  • Extend the key to be the length of the plaintext.
  • Use a Vigenère table to get the ciphertext.

• Example:
  • Plaintext: NINE ONE ONE AND ONE ONE TWO
  • Key: FOUR FOU RFO URF OUR FOU RFO
  • Ciphertext: SWHV TBY FSS UEI CHV TBY KBC
Plaintext: NINE ONE ONE AND ONE ONE TWO
Key: FOUR FOU RFO URF OUR FOU RFO
Ciphertext: SWHV TBY FSS UEI CHV TBY KBC
Plaintext:   NINE ONE ONE AND ONE ONE TWO
Key:        FOUR FOUR FOU RFO URF OUR FOU RFO
Ciphertext: SWHV TBY FSS UEI CHV TBY KBC
**Plaintext:**
NINE ONE ONE AND ONE ONE TWO

**Key:**
FOUR FOU RFO URF OUR FOU RFO

**Ciphertext:**
SWHV TBY FSS UEI CHV TBY KBC
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | A | A | A | C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| E | E | E | E | F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | F | F | G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | G | G | H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | H | H | I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | I | I | J | J | K | K | L | L | M | M | N | N | O | O | P | P | Q | Q | R | R | S | S | S | S | T | T | T | T |
| J | J | J | J | K | K | L | L | M | M | N | N | O | O | P | P | Q | Q | R | R | S | S | S | S | T | T | T | T | T | T |
| K | K | K | K | L | L | M | M | N | N | O | O | P | P | Q | Q | R | R | S | S | S | S | T | T | T | T | T | T | T | T |
| L | L | L | L | M | M | N | N | O | O | P | P | Q | Q | R | R | S | S | S | S | T | T | T | T | T | T | T | T | T | T |
| M | M | M | M | N | N | O | O | P | P | Q | Q | R | R | S | S | S | S | T | T | T | T | T | T | T | T | T | T | T | T |
| N | N | N | N | O | O | P | P | Q | Q | R | R | S | S | S | S | T | T | T | T | T | T | T | T | T | T | T | T | T | T |
| O | O | O | O | P | P | Q | Q | R | R | S | S | S | S | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T |
| P | P | P | P | Q | Q | R | R | S | S | S | S | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T |
| Q | Q | Q | Q | R | R | S | S | S | S | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T |
| R | R | R | R | S | S | S | S | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T |
| S | S | S | S | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T |
| T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T |
| U | U | U | U | V | V | V | V | W | W | W | W | X | X | X | X | Y | Y | Y | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z |

Plaintext: NINE ONE ONE AND ONE ONE TWO
Key: FOUR FOU RFO URF OUR FOU RFO
Ciphertext: SWHV TBY FSS UEI CHV TBY KBC
Plaintext:  NINE ONE ONE AND ONE ONE TWO
Key:  FOUR FOURFOU RFO URF OUR FOU RFO
Ciphertext:  SWHV TBY FSS UEI CHV TBY KBC
Vigenère Cipher
Vigenère Cipher

• To break:
  • Look for groups of three or more characters that regularly repeat.
  • Find a common factor for the distance between the repeating groups.
  • Perform frequency analysis on subsets of characters.

Key: ABCDABCDABCDABCDABCDABCDABCDABCD
Plaintext: CRYPTOISSHORTFORCRYPTOGRAPHY
Ciphertext: CSASTPKVSİQUTGQUCSASTPIUAQJB
Vigenère Cipher

• To break:
  • Look for groups of three or more characters that regularly repeat.
  • Find a common factor for the distance between the repeating groups.
  • Perform frequency analysis on subsets of characters.

Key:       ABCDABCDABCDABCDABCDABCD
Plaintext: CRYPTOISSHORTFORCRYPTOGRAPHY
Ciphertext: CSASTPKVIQUTGQUCSASTPIUAQJB
Transposition Ciphers

• These ciphers shift the original positions of each plaintext character. The ciphertext is just a permutation of the plaintext.
• Rail fence cipher
• Route cipher
Scytale

- Utilized by the Spartans of ancient Greece
- A strip of parchment would be wrapped around the scytale and the message written
- Both sides would need a scytale of the same diameter
- Easily breakable, the message itself hints at the encryption method
Rail Fence Cipher

• The plaintext is written downwards on “rails” of an imaginary fence, then written back upwards when the bottom is reached.

• Plaintext: WEAREDISCOVEREDFLEEATONCE

  W...E...C...R...L...T...E
  ..A...I...V...D...E...N..

• Ciphertext: WECRLTEERDSOEFEA0CAIVDEN
Rail Fence Cipher

• The plaintext is written downwards on “rails” of an imaginary fence, then written back upwards when the bottom is reached.

• Plaintext:  WEAREDISCOVEREDFLEEATONCE
  

• Ciphertext:  WECRLTEERDSOEEFEAOCAILVDEN
Rail Fence Cipher

• The plaintext is written downwards on “rails” of an imaginary fence, then written back upwards when the bottom is reached.

• Plaintext: WEAREDISCOVEREDFLEEATONCE

\[
W \ldots E \ldots C \ldots R \ldots L \ldots T \ldots E \\
E.R.D.S.O.E.E.F.E.A.O.C. \\
\]

• Ciphertext: WECKERLEERDSOOOEFEAOCAIVDEN
Rail Fence Cipher

• The plaintext is written downwards on “rails” of an imaginary fence, then written back upwards when the bottom is reached.

• Plaintext:   WEAREDISCOVEREDFLEEATONCE
   W...E...C...R...L...T...E
   ..A...I...V...D...E...N...

• Ciphertext: WECRLTEERDSOEEFEAOCAIVDEN
Rail Fence Cipher

• The plaintext is written downwards on “rails” of an imaginary fence, then written back upwards when the bottom is reached.

• Plaintext:  WEAREDISCOVEREDFLEEAATONCE
  WEAREDISCOVEREDFLEEAATONCE
  WEAREDISCOVEREDFLEEAATONCE
  WEAREDISCOVEREDFLEEAATONCE
  WEAREDISCOVEREDFLEEAATONCE
  WEAREDISCOVEREDFLEEAATONCE
  WEAREDISCOVEREDFLEEAATONCE
  WEAREDISCOVEREDFLEEAATONCE

• Ciphertext:  WECRLTEERDSOEFFEA0CAIVDEN
Rail Fence Cipher

- The plaintext is written downwards on “rails” of an imaginary fence, then written back upwards when the bottom is reached.
- Plaintext: WEAREDISCOVEREDFLEEAATONCE
  W...E...C...R...L...T...E
  ..A...I...V...D...E...N..
- Ciphertext: WECRLTEERDSOEEFEAOCIAIVDEN
Rail Fence Cipher

• The plaintext is written downwards on “rails” of an imaginary fence, then written back upwards when the bottom is reached.

• Plaintext:  WEAREDISCOVEREDFLEETONCE

  W...E...C...R...L...T...E


  ..A...I...V...D...E...N..

• Ciphertext:  WECRLTEERDSOEEFEAOCAIVDEN
Rail Fence Cipher

• The plaintext is written downwards on “rails” of an imaginary fence, then written back upwards when the bottom is reached.

• Plaintext: WEAREDISCOVEREDFLEEATONCE

  W...E...C...R...L...T...E
  E.R.D.S.O.E.E.F.E.A.O.C.
  ..A...I...V...D...E...N...

• Ciphertext: WECRLTEERDSOEEFEAOCAIVDEN
Route Cipher

• The plaintext is written on a grid of given dimensions and padded with low-frequency characters.

```
W R I O R F E O E
E E S V E L A N J
A D C E D E T C X
```

• The key is how you derive the ciphertext: “Spiral counter-clockwise, starting from the top right.”

• Ciphertext: **EOEFROIRWEADCEDETCXJNALEVSE**
Route Cipher

• The plaintext is written on a grid of given dimensions and padded with low-frequency characters.

```
W R I O R F E O E
E E S V E L A N J
A D C E D E T C X
```

• The key is how you derive the ciphertext: “Spiral counter-clockwise, starting from the top right.”

• Ciphertext: **EOEFROIRWEADCEDETCXJNALEVSE**
Route Cipher

• The plaintext is written on a grid of given dimensions and padded with low-frequency characters.

W R I O R F E O E
E E S V E L A N J
A D C E D E T C X

• The key is how you derive the ciphertext: “Spiral counter-clockwise, starting from the top right.”

• Ciphertext: E O E F R O I R W E A D C E D E T C X J N A L E V S E
Route Cipher

• The plaintext is written on a grid of given dimensions and padded with low-frequency characters.

W R I O R F E O E
E E S V E L A N J
A D C E D E T C X

• The key is how you derive the ciphertext: “Spiral counter-clockwise, starting from the top right.”

• Ciphertext:  EOEFROIRWEADCEDETCXJNALEVSE
Route Cipher

• The plaintext is written on a grid of given dimensions and padded with low-frequency characters.

\[
\begin{array}{cccccccc}
W & R & I & O & R & F & E & O & E \\
E & E & S & V & E & L & A & N & J \\
A & D & C & E & D & E & T & C & X \\
\end{array}
\]

• The key is how you derive the ciphertext: “Spiral counter-clockwise, starting from the top right.”

• Ciphertext: \textbf{EOEFROIRWEADCEDETCXJNALEVSE}
Route Cipher

• The plaintext is written on a grid of given dimensions and padded with low-frequency characters.

W R I O R F E O E
E E S V E L A N J
A D C E D E T C X

• The key is how you derive the ciphertext: “Spiral counter-clockwise, starting from the top right.”

• Ciphertext:  **EOEFROIRWEADCEDETCXJNALEVSE**
Route Cipher

• The plaintext is written on a grid of given dimensions and padded with low-frequency characters.

```
  W R I O R F E O E
  E E S V E L A N J
  A D C E D E T C X
```

• The key is how you derive the ciphertext: “Spiral counter-clockwise, starting from the top right.”

• Ciphertext:  

```
EOEFROIWEADCEDETCXJNALEVSE
```
Route Cipher

• The plaintext is written on a grid of given dimensions and padded with low-frequency characters.

  W R I O R F E O E
  E E S V E L A N J
  A D C E D E T C X

• The key is how you derive the ciphertext: “Spiral counter-clockwise, starting from the top right.”

• Ciphertext:  EOEFROIRWEADCEDETCXJN ALEVSE
Route Cipher

• The plaintext is written on a grid of given dimensions and padded with low-frequency characters.

```
W R I O R F E O E
E E S V E L A N J
A D C E D E T C X
```

• The key is how you derive the ciphertext: “Spiral counter-clockwise, starting from the top right.”

• Ciphertext: **EOEFROIRWEADCEDETCXJNALEVSE**
Modern Cryptography

- Cryptography was greatly changed by the use of first analog then digital computers
  - More complex algorithms
  - Easier to break algorithms
- Increased focus on mathematics
  - Messages had to be machine readable
Encodings

- With computers messages are now in binary
  - Binary represented in different ways for humans to understand
- Different character sets such as ASCII, Unicode
- Hex: Uses base 16 numbers to avoid long strings of binary
- Base64: Uses base 64 numbers to condense it further

Examples:

- ASCII - hello
- Binary - 01101000 01100101 01101100 01101100 01101111
- Hex - 0x68 0x65 0x6c 0x6c 0x6f
- Base64 - aGVsbG8
XOR

- Common operation in computers
- Allows use to manipulate binary bits based on an input
- If $A$ is plaintext and $C$ is ciphertext, then we can use XOR to encrypt and decrypt a message using key $B$

$$(A \text{ XOR } B = C) \iff B \text{ XOR } C = A$$

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>$A \text{ XOR } B$</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

- Achieves perfect secrecy, provides no information on the plaintext
  - Only if key same length as the message
- Adds each symbol in plaintext with corresponding symbol in the key

With ROT13:

```
HELLO
+ + + + +
AVVYYB
```

With One Time Pad:

```
HELLO
AFPGE
V V V V V
HJARS
```
CIPHERTEXT: HJARS, HULGO, SFAPL

KEY: HULGO

PLAINTEXT: APPLE, PEACH
One Time Pad Usage

- Used during the Cold War
  - Allowed for secure communication later on an unsecured channel
- Requires the key to be securely distributed in advance
  - Key can also be used only once
- Distribution of a key the same length of the message is difficult
  - How could you make it work with a smaller key?
Modern Cipher Categories

**Symmetric**
- Uses a shared secret key to encrypt and decrypt messages
- Requires the key to be distributed in a secure manner

**Asymmetric**
- Uses a two separate, mathematically related keys to encrypt and decrypt
  - A message encrypted with one key can only be decrypted with the other
- Each person will have a public/private keypair
Symmetric Key Encryption

- Shared key is used in the cipher algorithm
  - Different algorithms such as DES, AES
- Requires the key to be distributed securely
- Can generate more keys based off the original secret key
- Relatively quick
- Used in the majority of communication encryption schemes
Asymmetric Key Encryption

- A pair of related keys are generated in advance for each user
- Private key is kept secret, public key is shared
- Any message encrypted with the public key can only be decrypted with the private key, and vice versa
- Encryption is relatively slow and complex
- Used for symmetric key distribution and authentication
Integrity
Cryptography and Computers

- Introduction of computers changed how cryptography is done
- Also introduced new uses for cryptography
- The fast computation allowed for values to be quickly generated based on message contents
- This value can be created at both sender and receiver, then compared
Hash Functions

- One-way algorithm
- Given any input of any length, produces a string of a given length $n$
- Used for integrity, message digests, and password storage

```
Input: Fox → Hash function → DFCD3454
Input: The red fox runs across the ice → Hash function → 52ED879E
Input: The red fox walks across the ice → Hash function → 46042841
```
Properties of Good Hash Functions

- Impossible to reverse
- Output is always of a fixed size
- Changing any part of the input changes the hash completely
- Hard to find collisions, where two inputs give the same output
Authentication
Proving Who You Are

- Communication is done increasingly digitally
- Difficult to tell if someone really is who they say they are
- Cryptography provides us tools that can be used to prove someone's identity
- Prove by:
  - Knowing a secret only the person would know
  - Telling you something in a way only the person could
Known Shared Secret

- Prove who you are by knowing something, i.e. a password
- By comparing with a stored value, you can authenticate
- Don’t compare against the plain password
- Add salt for extra flavour
  - And security
Symmetric Encryption

- Prove identity by sending a message encrypted with the shared key
- Only the people who know the secret key should be able to use it
- Anyone who sends a recognizable message should be the person they say they are
  - Or are they?
Asymmetric Encryption

- With an asymmetric key pair, any message encrypted with the private key can only be decrypted with the public key.
- Since only the person should know their private key, only they could send a message.
- Must make sure the public key is valid.
Conclusion
Cryptography In The Future

- Quantum computers will eventually change the algorithms we use
- Continue to find ways to securely communicate
  - And validate life choices of math majors
- Questions?