Cryptography

- **Cryptography** (from Greek "kryptós" = "hidden, secret" and "graphein" = "writing") is the practice and study of techniques for secure communication in the presence of third parties called adversaries.
- More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.
- Relates to **computer security**: data confidentiality, data integrity

https://en.wikipedia.org/wiki/Cryptography
Cryptography

- Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics.
- Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

https://en.wikipedia.org/wiki/Cryptography
Eavesdropping
In Cryptography, the idea is to make Eavesdropping ineffective/difficult.
In Cryptography, the idea is to make Eavesdropping ineffective/difficult.

Sender/Receiver

Bob

Kyle

Eavesdropper

Eavesdropping

Sender/Receiver

Alice
Terminology

- **Plaintext** is the text of the original, non-hidden message that the sender desires to communicate to the receiver
- **Ciphertext** is the hidden text, that the plaintext is converted to during message transmission
- **Encrypt**: Plaintext $\rightarrow$ Ciphertext conversion
- **Decrypt**: Ciphertext $\rightarrow$ Plaintext conversion
Cryptography

- Very simple cryptography has been in use for millennia
- Known to have been used by:
  - Hebrew Scholars (600 BC)
  - In India (400 BC)
- One of the earliest known forms of this is known as a substitution cipher
Substitution Cipher

- A cipher is “a secret or disguised way of writing; a code”
- It requires a pair of algorithms
  - one that creates the encrypted message (the ciphertext)
  - one that reverses the encryption (the plaintext)
- A substitution cipher is one in which the numbers and letters in a message are replaced by pre-determined other letters/numbers
Substitution Cipher

For example, could use this rule:
To convert plaintext to ciphertext, replace
  A->B,  B->C,  C->D,  D->E,  . . .  X->Y,  Y->Z,  Z->A
Substitution Cipher

For example, could use this rule:
To convert plaintext to ciphertext, replace
   A->B,  B->C,  C->D,  D->E,  . . .  X->Y,  Y->Z,  Z->A

Encrypt the following message: “HOW ARE YOU”
Substitution Cipher

For example, could use this rule:
To convert plaintext to ciphertext, replace
  A->B, B->C, C->D, D->E, ... X->Y, Y->Z, Z->A

Encrypt the following message: “HOW ARE YOU”

"IPX  BSD  ZPV"
Substitution Cipher

For example, could use this rule:
To convert plaintext to ciphertext, replace
   A->Z, B->A, C->B, D->C . . .
Substitution Cipher

For example, could use this rule:
To convert plaintext to ciphertext, replace
  A->Z, B->A, C->B, D->C . . .

Decrypt the following message: “HPPECZF”
Substitution Cipher

For example, could use this rule:
To convert plaintext to ciphertext, replace
   A->Z, B->A, C->B, D->C . . .

Decrypt the following message: “HPPECZF”
  "GOODBYE"
Substitution Cipher

- In the prior example, we substituted each letter with corresponding “shifted” letter using a 1-letter shift
- Specifically called **Caesar cipher**
- Can do this with other shift amounts too
Substitution Cipher

- In the prior example, we substituted each letter with corresponding “shifted” letter using a 1-letter shift
- Specifically called **Caeser cipher**
- Can do this with other shift amounts too
- Helps to write out the shifted alphabet when doing translations:
Caesar Cipher

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
Caesar Cipher

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 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
Caesar Cipher

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 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

25
Caesar Cipher
Caesar Cipher

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

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

This is a 1-shift
Caesar Cipher Encryption

How about a 3-shift?
Caesar Cipher Encryption

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
Caesar Cipher Encryption

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 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

↑↑↑↑

↓↓↓↓
Caesar Cipher Encryption

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

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
This is a 3-shift

Caesar Cipher Encryption
## Exercise

Decrypt the following messages

<table>
<thead>
<tr>
<th>Using a 5-letter shift:</th>
<th>Using a 4-letter shift:</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAJWD FWYNXY BFX</td>
<td>EVXSS HIIXSS ERH WII</td>
</tr>
<tr>
<td>KNWXY FS FRFYZJW</td>
<td>XLVIITMS</td>
</tr>
</tbody>
</table>
Exercise

Each table:

- Make up a short message (4 words max)
- Encrypt the message, and put the result on a whiteboard
  - Make sure to also put the shift amount on the board!
Exercise

Each table:
- Make up a short message (4 words max)
- Encrypt the message, and put the result on a whiteboard
  - Make sure to also put the shift amount on the board!
Exercise

Each table:

- Make up a short message (4 words max)
- Encrypt the message, and put the result on a whiteboard
  - Make sure to also put the shift amount on the board!
Exercise

Each table:

● Make up a short message (4 words max)
● Encrypt the message, and put the result on a whiteboard
  ○ Make sure to also put the shift amount on the board!
● Once everyone’s done, pass your whiteboard to another table and accept another whiteboard
● Decrypt the message you receive
Rail Cipher

- A *rail cipher* is one in which the letters of the plaintext are arranged on N-character tall “rails” and then converted to ciphertext (Think of the rail as rows.)
- The plaintext is written on alternate rails (or rows) in a zigzag pattern.
- Let's do an example.
Rail Cipher

- Want to send the message “WELCOME TO COMPUTER SCIENCE” encrypted with a 3-rail cipher
Rail Cipher

- Want to send the message “WELCOME TO COMPUTER SCIENCE” encrypted with a 3-rail cipher
- To do this, write each letter in a different rail in a 3-level zig-zag pattern:
Want to send the message “WELCOME TO COMPUTER SCIENCE” encrypted with a 3-rail cipher
To do this, write the letters in a 3-level zig-zag pattern:
Rail Cipher

- The message “WELCOME TO COMPUTER SCIENCE” can be drawn on a 3-rail grid as shown below

```
```
Rail Cipher

- The message “WELCOME TO COMPUTER SCIENCE” can be drawn on a 3-rail grid as shown below.
- Notice the up/down pattern.
Rail Cipher

- The message “WELCOME TO COMPUTER SCIENCE” can be drawn on a 3-rail grid as shown below.
- Then “squish” the text together along the rows, from left-to-right, to create the ciphertext.
Rail Cipher

- The message “WELCOME TO COMPUTER SCIENCE” can be drawn on a 3-rail grid as shown below
- This gives “WOTOTSNECM OCMUE CECLE PRIE”
Rail Cipher

- Can make N-tall rails (where N is any number greater than 2) to hide messages

```
3-Rail

4-Rail
  . . . . . . . . . . C . . . . . . O . . . . . U . . . . . C

2-Rail
```
• Write the ciphertext for the plaintext message using the 4-rail cipher
Rail Cipher - decryption

- If the receiver of the message has the ciphertext and knows the number of rails that the sender used to encrypt, can decrypt the message by reverse-constructing the rails.
- Start by making as many rows as there are keys.
- The number of columns is the length of the ciphertext.
- Write out the ciphertext in the pattern dictated by the key and number of rails, in a zig zag fashion.
- Let's do an example.
Rail Cipher - decryption

- This is a 3-rail cipher
- The ciphertext is “WOTOTSNECM OCMUE CECLE PRIE”
- It has length 27
Rail Cipher - decryption

- This is a 3-rail cipher
- The ciphertext is “WOTOTSNECM OCMUE CECLE PRIE”
- It has length 27
- We place the W in the first row/column

```
W
```

```
Rail Cipher - decryption

- This is a 3-rail cipher
- The ciphertext is “WOTOTSNECM OCMUE CECLE PRIE”
- It has length 27
- We place the W in the first row/column
- Then place dashes down and up until you reach the top row again
Rail Cipher - decryption

- This is a 3-rail cipher
- The ciphertext is “WOTOTSNECM OCMUE CECLE PRIE”
- It has length 27
- We place the W in the first row/column
- Then place dashes down and up until you reach the top row again
- Then place the next character O. Repeat.
Rail Cipher - decryption

- This is a 3-rail cipher
- The ciphertext is “WOTOTSNCECM OCMUE CECLE PRIE”
- It has length 27
- We place the W in the first row/column
- Then place dashes down and up until you reach the top row again
- Then place the next character O. Repeat.
Rail Cipher - decryption

- This is a 3-rail cipher
- The ciphertext is “WOTOTSNECM OCMUE CECLE PRIE”
- It has length 27
- Now place the E in the second row
Rail Cipher - decryption

- This is a 3-rail cipher
- The ciphertext is “WOTOTSNECM OCMUE CECLE PRIE”
- It has length 27
- Now place the E in the second row
Rail Cipher - decryption

- This is a 3-rail cipher
- The ciphertext is “WOTOTSNECM OCMUE CECLE PRIE”
- It has length 27
- Now place the E in the second row
- Go down and up until you hit the second row again
- Then place C

```
. . - . . . - . . . - . . . - . . . - . . . - . . . - . . . -
```
Rail Cipher - decryption

- This is a 3-rail cipher
- The ciphertext is “WOTOTSNECM OCMUE CECLE PRIE”
- It has length 27
- Now place the E in the second row
- Go down and up until you hit the second row again
- Then place C

```
. . - . . . - . . . - . . . - . . . - . . . - . . . -
```
Rail Cipher - decryption

- This is a 3-rail cipher
- The ciphertext is “WOTOTSNECM OCMUE CECLE PRIE”
- It has length 27
- Where will M go?
Rail Cipher - decryption

- This is a 3-rail cipher
- The ciphertext is “WOTOTSNECM OCMUE CECLE PRIE”
- It has length 27
- Where will M go?
- In the dashed spot on the second row
Rail Cipher - decryption

- This is a 3-rail cipher
- The ciphertext is “WOTOTSNECM OCMUE CECLE PRIE”
- It has length 27
- Where will M go?
- In the dashed spot on the second row
Rail Cipher - decryption

- This is a 3-rail cipher
- The ciphertext is “WOTOTSNECM_OCMUE_CECLE_PRIE”
- It has length 27
- Fill out the rest!

```
```
Rail Cipher

- Create a 3-Rail cipher for this text: “Star Wars: The Last Jedi”
Rail Cipher

- Create a 3-Rail cipher for this text: “Star Wars The Last Jedi”

```
```
Rail Cipher

• Decrypt the following ciphertext using a 4-rail cipher:
• “WE NDHVRUDOTA SAE OOD ETITY RH”
Rail Cipher

- Decrypt the following ciphertext using a 4-rail cipher: “WE NDHVRUDOTA SAE OOD ETITY RH”

WHATEVER YOU DO DON’T READ THIS
## Exercise

Do the following using rail-ciphers

<table>
<thead>
<tr>
<th>Decrypt with 2-rail cipher:</th>
<th>Decrypt with 3-rail cipher:</th>
<th>Encrypt with 4-rail cipher:</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMATETLZOPRMNAIE</td>
<td>RFEHALECCPEINIR</td>
<td>YOU NEED A HIGH FIVE TODAY</td>
</tr>
</tbody>
</table>
Exercise

Each table:

- Make up a short message (4 words max)
- Encrypt the message using 3-rail cipher, and put the result on a whiteboard
Exercise

Each table:

• Make up a short message (4 words max)
• Encrypt the message using 3-rail cipher, and put the result on a whiteboard
• Once everyone’s done, pass your whiteboard to another table and accept another whiteboard
• Decrypt the message you receive
Materials

• Required Materials
    ▪ Specifically: Four-square, Baconian
  ○ UTDW chapter 12