Cybersecurity and Encryption

Reese Hatfield

Cybersecurity

- We’ve worked with a lot of data
- Data
  - All binary at the end of the day
  - Doing something to the hardware
- Data is important
- Your life revolves around “data”

Cybersecurity

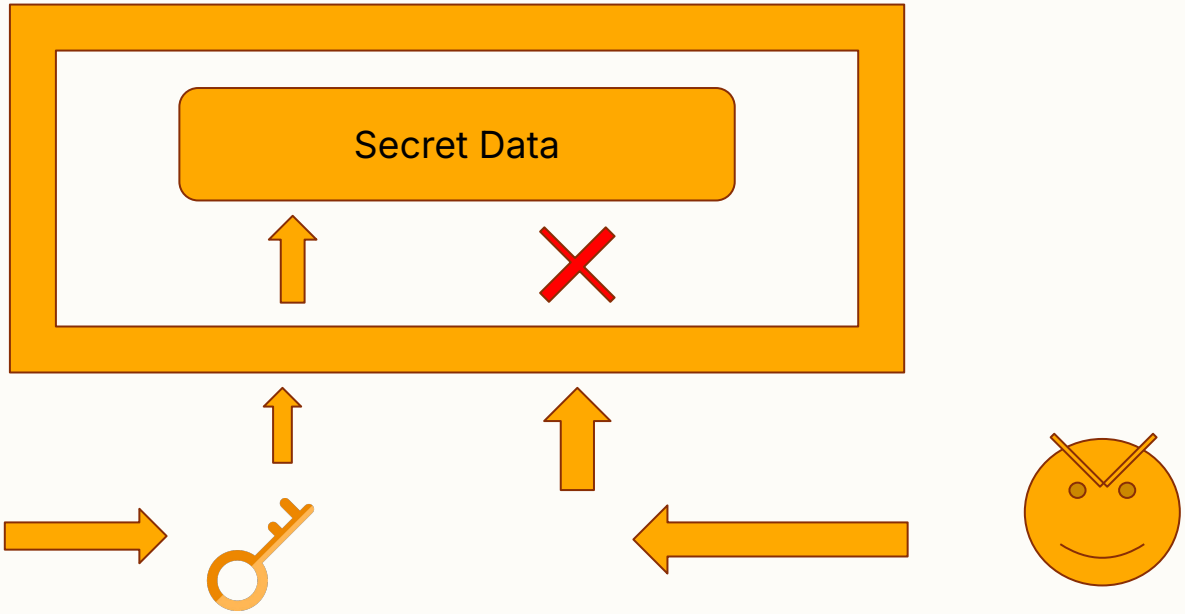
- Data is so important
  - That is should protected in some form
- How can secure our data?
- Especially at the software level?
- What do I mean by “secure”?

Cybersecurity

- Easily accessible to me
- But NOT anyone else
- Take some piece of information
- Hide it
- But with something only I know

Cybersecurity

- Conceptual Model



Cybersecurity

- Encode our data
- Special representation
- Split our data into two pieces
  - Key
  - Hidden Text
- We can use the key to “unlock” the hidden information

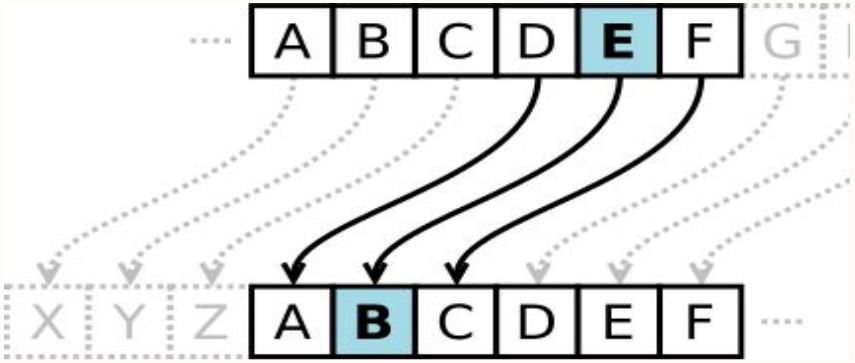
Cybersecurity

- Oftentimes, the “key” is just the knowledge of how to decode the text
  - But can be arbitrary data

- Let’s look at one of the earliest examples of hidden message encoding

Cybersecurity

- Caesar Cipher
- Julius Caesar supposedly used this
- Move all the characters over by some amount
- Cycling back around when out of space



Encoding with Caesar

- Key = how much to shift by
- Key = 3
- H E L L O

- K H O O R

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				

Encoding with Caesar

- Key = how much to shift by
- Key = 4
- B Y T E
  Plaintext

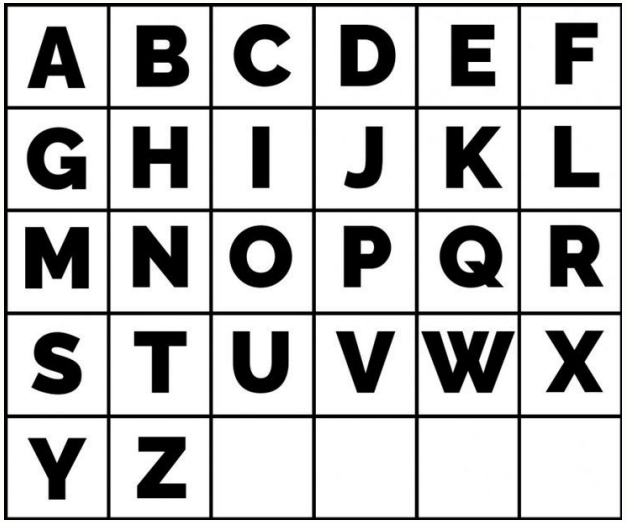
- F C X I
  Ciphertext
  Wraps around

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				

Encoding with Caesar

- Key = how much to shift by
- Key = -2
- B O B
  Plaintext

- Z M Z
  Ciphertext
  Goes backwards



Decoding with Caesar

- Key = how much to shift by
- Key = ?
- G P Y
  Ciphertext Worthless w/o key
- Key = +1
- F O X

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				

Route Cipher

- We can also encode in other ways
- “Route Cipher”
- Write out message in a box
- Spiral around the box to encode the message
- De-Spiral to decode the message
- Key = The “route” we take around the box

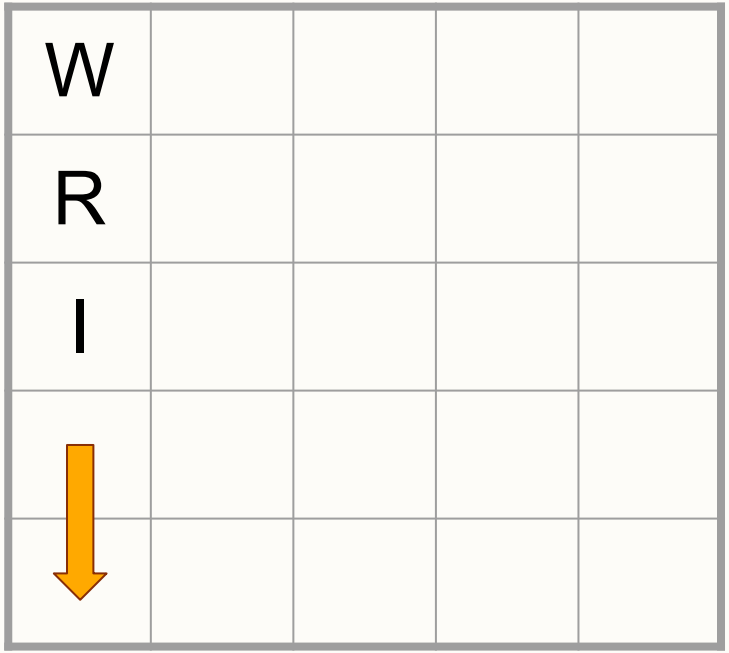
Route Cipher

- Pick a square that fits your message
- Write it out top down

- “WRIGHT STATE UNIVERSITY”
- 5×5 Grid
- ~25 characters
- As long as it fits

Route Cipher

- Start in top left
- Work down
- “WRIGHT STATE UNIVERSITY



Route Cipher

- Start in top left
- Work down
- “WRIGHT STATE UNIVERSITY

W	T			
R				
I				
G				
H				

Route Cipher

- Start in top left
- Work down
- “WRIGHT STATE UNIVERSITY

W	T	E	E	
R	S	U		
I	T	N		
G	A	I		
H	T	V		

Route Cipher

- Start in top left
- Work down
- “WRIGHT STATE UNIVERSITY

W	T	E	E	Y
R	S	U	R	?
I	T	N	S	?
G	A	I	I	?
H	T	V	T	?

Route Cipher

- “WRIGHT STATE UNIVERSITY
- Pad with some extra symbol
- Can be anything

W	T	E	E	Y
R	S	U	R	?
I	T	N	S	?
G	A	I	I	?
H	T	V	T	?

Route Cipher

- “WRIGHT STATE UNIVERSITY
- Pad with some extra symbol
- Can be anything

W	T	E	E	Y
R	S	U	R	X
I	T	N	S	X
G	A	I	I	X
H	T	V	T	X

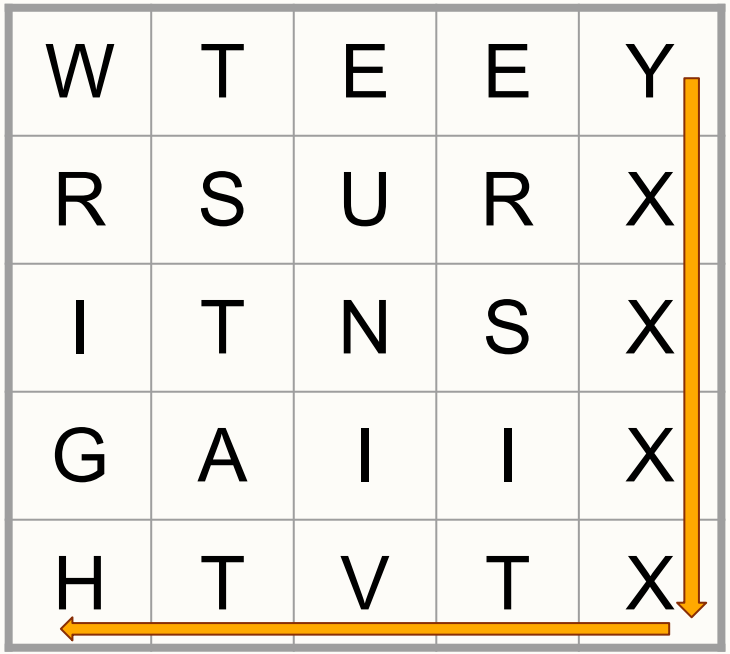
Route Cipher

- Follow around the block in a spiral pattern
- Write down as you go

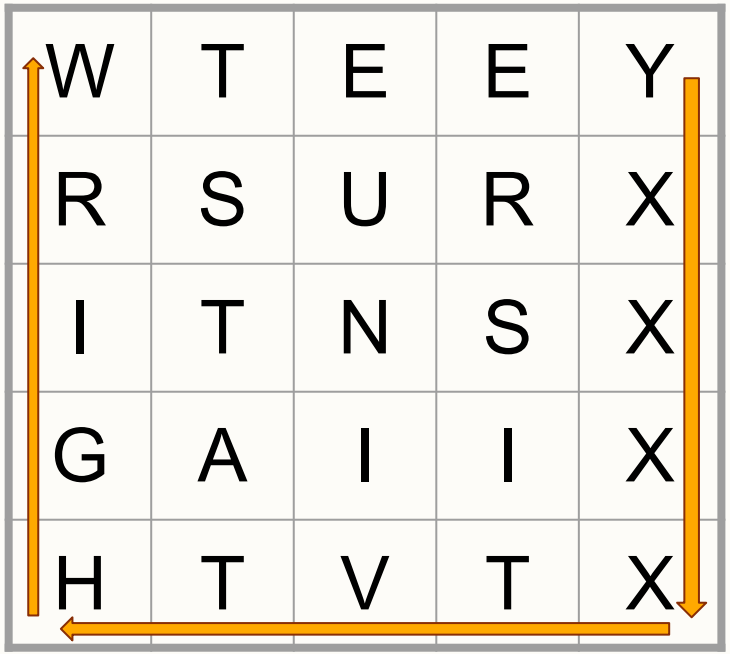
W	T	E	E	Y
R	S	U	R	X
I	T	N	S	X
G	A	I	I	X
H	T	V	T	X

W	T	E	E	Y
R	S	U	R	X
I	T	N	S	X
G	A	I	I	X
H	T	V	T	X

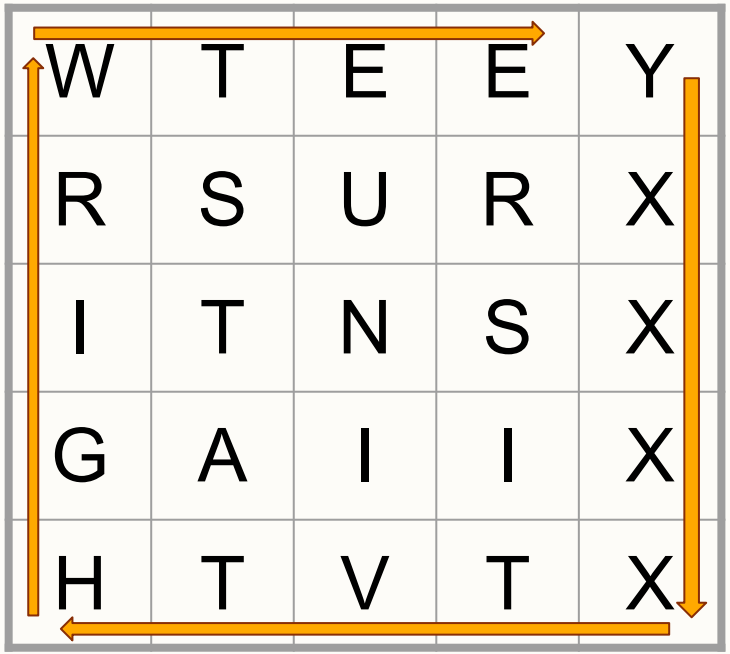
Encoded Message: **YXXXX**



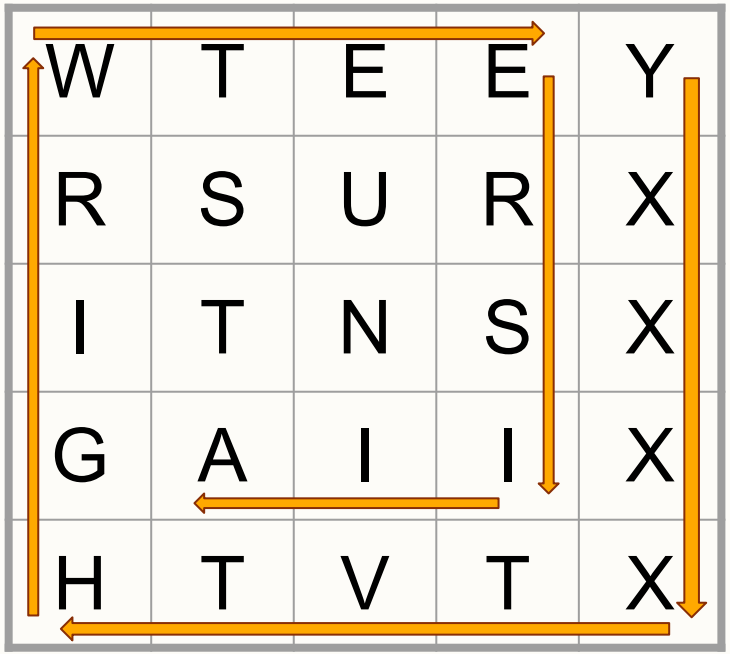
Encoded Message: **YXXXXTVTH**



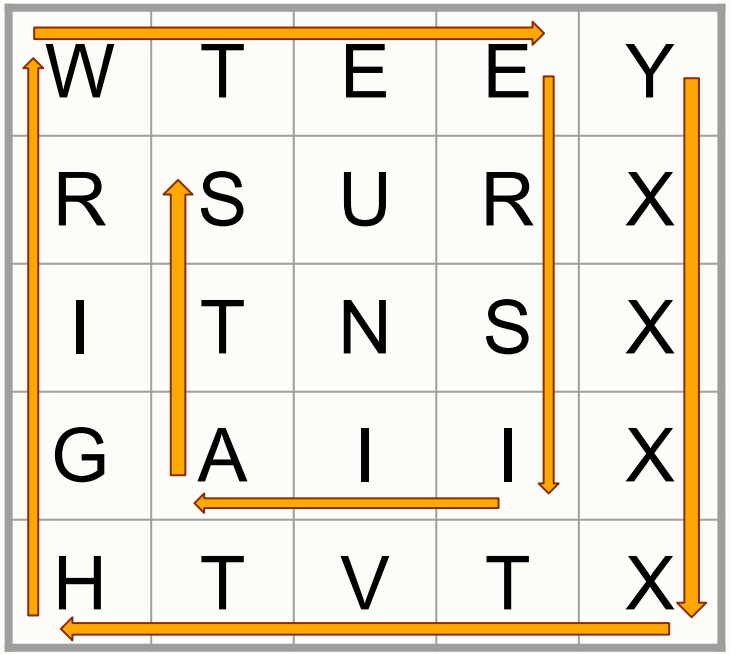
Encoded Message: **YXXXXTVTHGIRW**



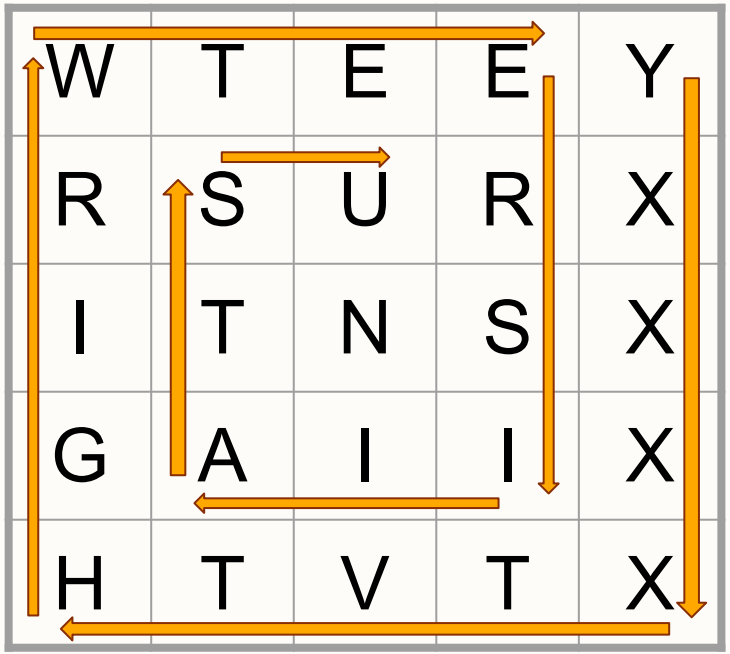
Encoded Message: **YXXXXTVTHGIRWTEE**



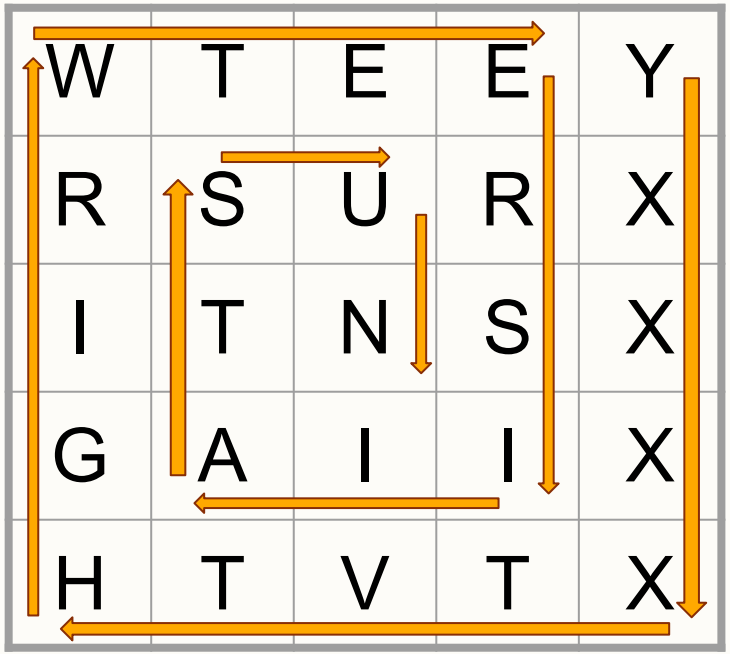
Encoded Message: **YXXXXXTVTHGIRWTEERSIIA**



Encoded Message: **YXXXXXTVTHGIRWTEERSIIAST**



Encoded Message: **YXXXXTVTHGIRWTEERSIIASTU**



Encoded Message: **YXXXXTVTHGIRWTEERSIIASTUN**

Route Cipher

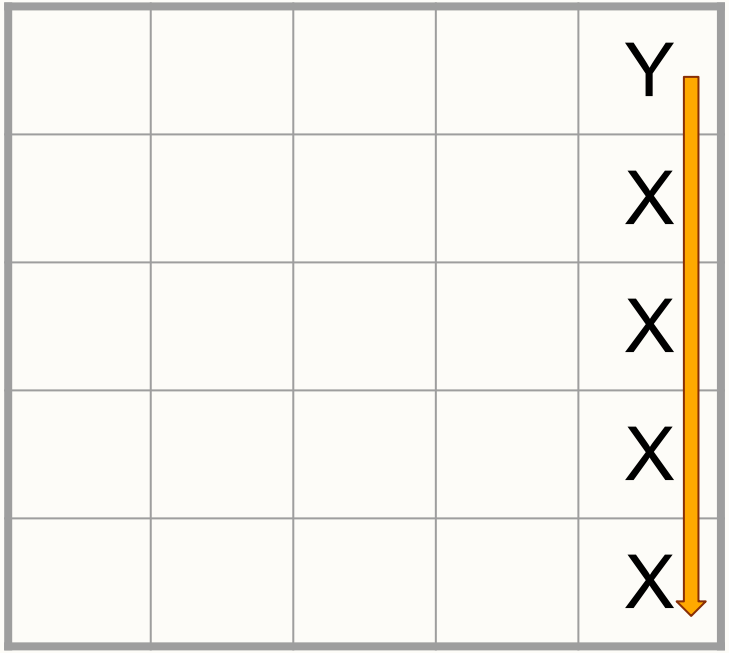
- This message is incomprehensible*
- But if you
  - Know a route cipher was used
  - Know how it was originally written
  - Know how to spiral (start location, direction)
- This knowledge becomes your key
  - Let’s decode it

Route Cipher

- Start by writing it out in the same direction we spiraled in
  - I.e. top left, down + around

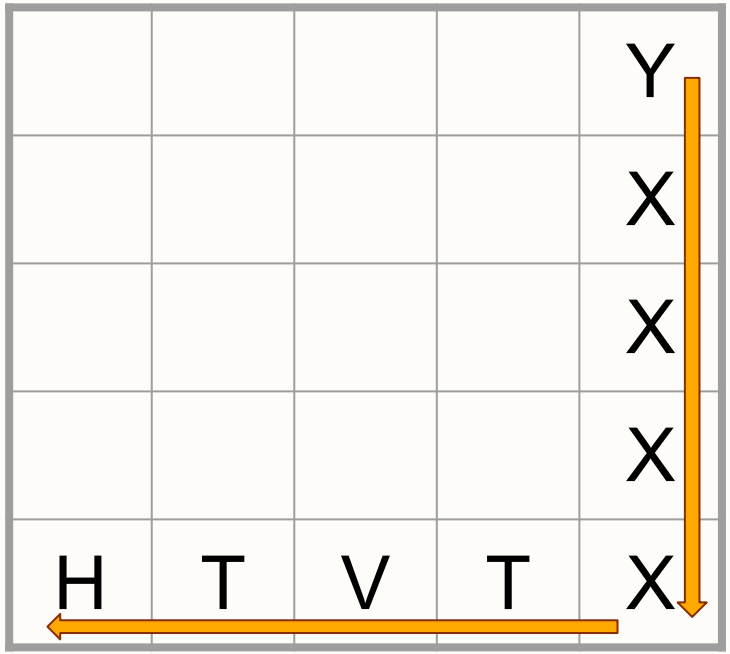
- Then read it the same way we originally wrote it
  - I.e. top down

Encoded Message: **YXXXX**TVTHGIRWTEERSIIASTUN



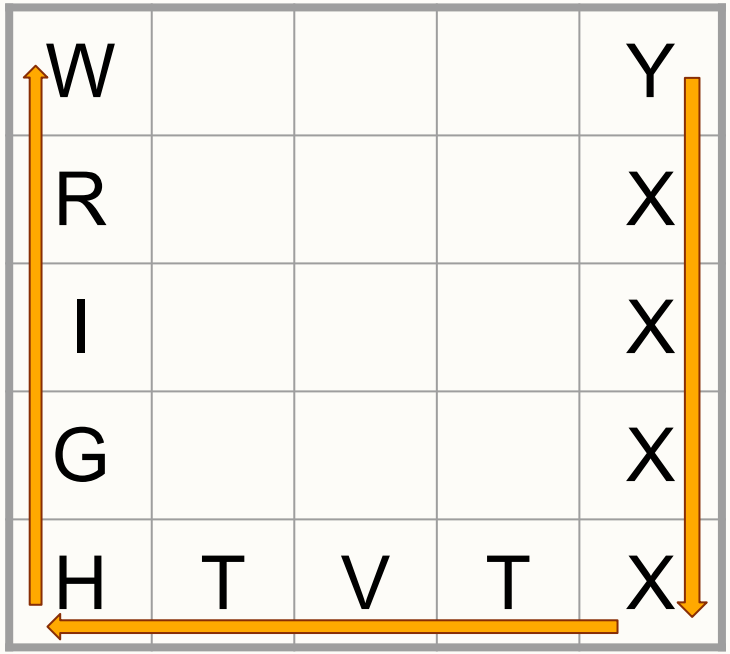
Decoded Message:

Encoded Message: **YXXXXTVTH**GIRWTEERSIIASTUN



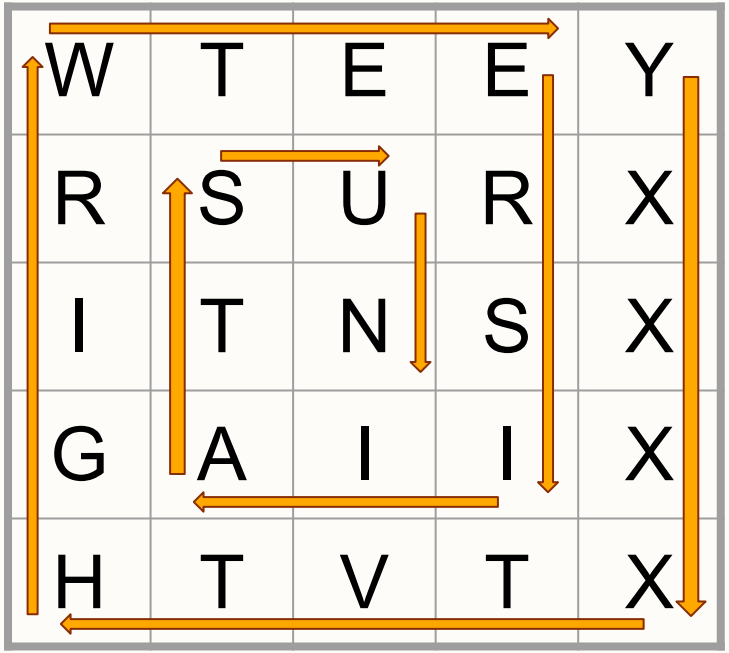
Decoded Message:

Encoded Message: **YXXXXTVTHGIRW**TEERSIIASTUN



Decoded Message:

Encoded Message: **YXXXXTVTHGIRWTEERSIIASTUN**



Decoded Message:

Encoded Message: **YXXXXXTVTHGIRWTEERSIIASTUN**

- After the spiral is done
- Go down our originally direction

W	T	E	E	Y
R	S	U	R	X
I	T	N	S	X
G	A	I	I	X
H	T	V	T	X

Decoded Message:

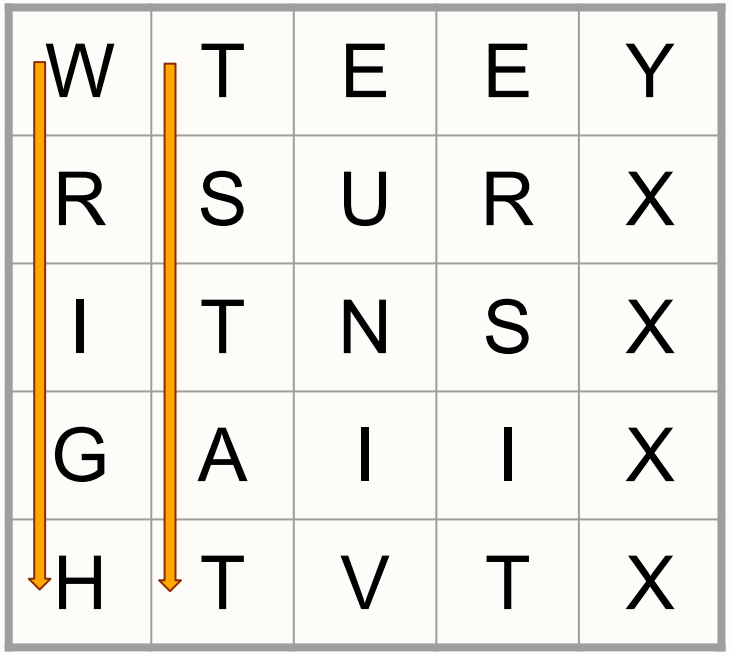
Encoded Message: **YXXXXXTVTHGIRWTEERSIIASTUN**

- After the spiral is done
- Go down our originally direction

+Decoded Message: **WRIGH**

Encoded Message: **YXXXXXTVTHGIRWTEERSIIASTUN**

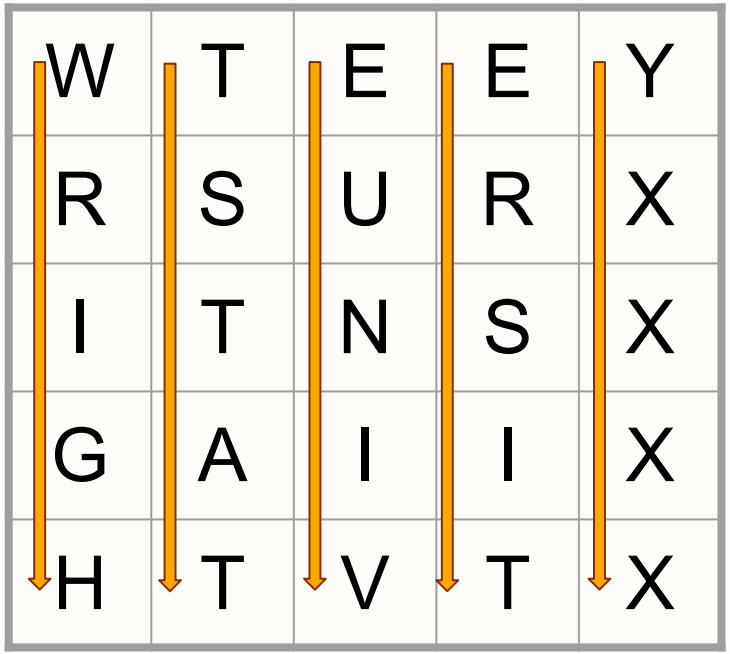
- After the spiral is done
- Go down our originally direction



+Decoded Message: **WRIGHTSTAT**

Encoded Message: **YXXXXXTVTHGIRWTEERSIIASTUN**

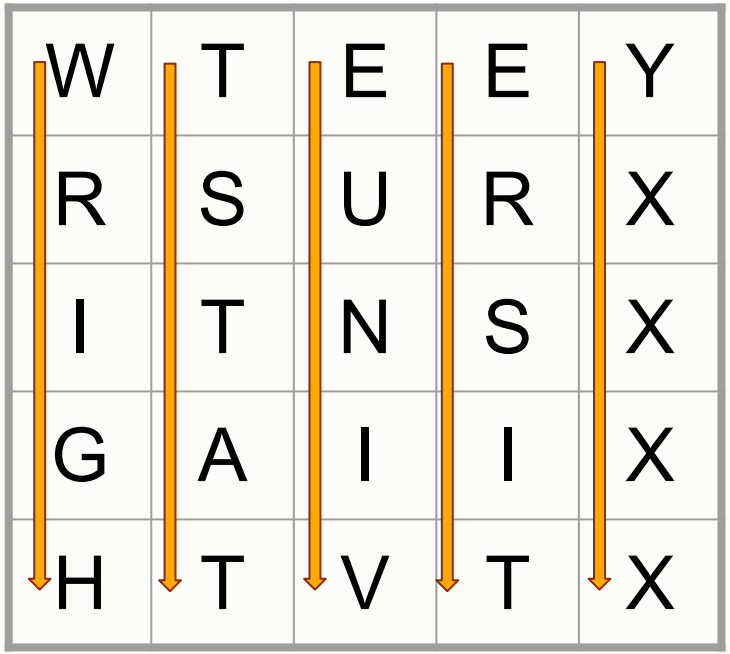
- After the spiral is done
- Go down our originally direction



+Decoded Message: **WRIGHTSTATEUNIVERSITYXXXX**

Decoded Message: **WRIGHTSTATEUNIVERSITYXXXX**

- We still have our leftover symbols at the end
- Ensure that know this symbol ahead of time



Cipher

- There are many types of ciphers
- The ones we have seen
  - Are not very good
  - Insecure
  - Easy to “crack”
- There are *much* better was of doing this

Cipher

- Hiding information like this is referred to as “encrypting”
- Un-hiding information like this is referred to as “decrypting”