Frank Cash

#### Who Am I?

• https://frankcash.github.io/

• Twitter: @hackthethings

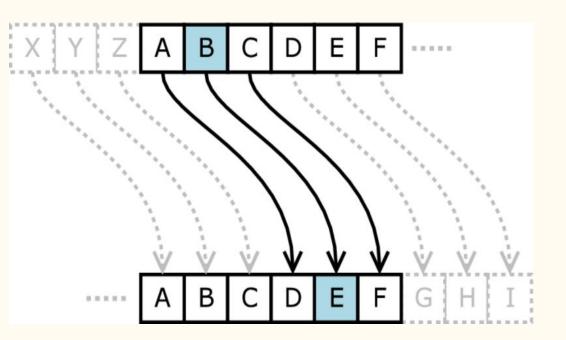
• Github: @frankcash



• Terms

• History of Selected Ciphers

• Example Ciphers



• Terms

• History of Selected Ciphers

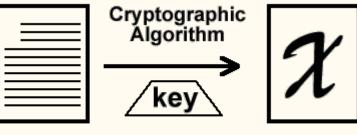
• Example Ciphers

#### Terms

• Plaintext

• Cipher

• Ciphertext



plaintext

ciphertext

• Terms

• History of Selected Ciphers

• Example Ciphers

### History of Selected Ciphers

• Rotation Ciphers

• Transposition Cipher

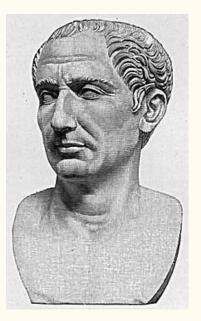
• Nihilist Ciphers

#### **Rotation Ciphers**

• Not the First Cipher Used

• Used by Caesar

• Common Sub-Cipher



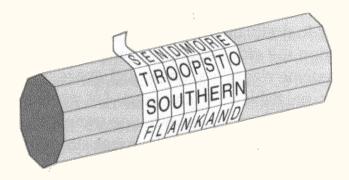


#### Transposition Cipher

• Scytale Used by Greeks

• Used During Civil War

• Strengthens Weak Ciphers

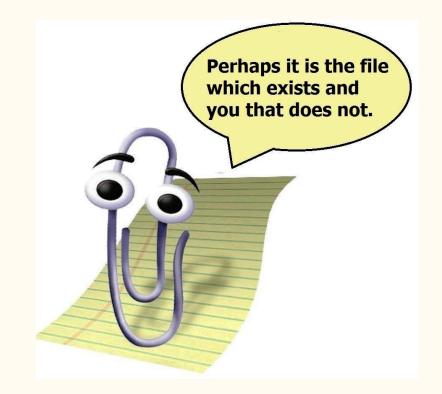


#### Nihilist Ciphers

• Symmetric Encryption

• Russian Nihilists (1880s)

• Soviet Spies (WWII - Cold War)



• Terms

• History of Selected Ciphers

• Example Ciphers

### Example Ciphers

• Vigenere Cipher

• Route Cipher

• VIC Cipher

## Vigenere Cipher

• Complex Substitution Cipher

• Builds on Caesar Shift

• Commonly Used in CTFs

• Utilizes a Key

### Vigenere Cipher

• Utilize Vigenere Table

• Encrypting: Row (Plaintext) -> Column (Key) = Ciphertext

• Decrypting: Column (Key) -> Row (Ciphertext) Output = Plain(text)

KLMNOPOR A A B C HIKE O = P88 K L M N O P O R CCDEF I J K L M N O P Q R S T U V W X G H DDEF HIJKLMNOPORSTUVWX MNOPORSTUVW Ο. 18. ю. RSTUVW N O P ORSTUVWXY  $M \rightarrow M$ ZA 8 STUVWXY CD 8. LMNOPORSTUVWX YZABCDE UVWXYZABCDE GIN £Ω. D. ie. 8 c. G H PPO B D. EF GH ю. **B**: DEFGH 0.P E. GHIIK GHI L K L Gr. - K 1 医上层 GHIIKLMNOP GHIJKLMNOPORS WWXYZ E. IKLMNOPOR YYZABCD GHIJKLMNOPORSTU E. ZZABCDEFGHIJKLMNOPORSTUVWXY

### Vigenere Cipher

• Plaintext: A Game. A Movie Star.

• Key (Repeats): Pragyan

• Ciphertext: p xasc. a zdmik qtng.

AAB 88 **D**. CCD E IKLMNOPORSTUV 8 DDE MNOPQRSTUV PORSTU Ю. GG  $\mathbb{O}^{1}$ O. 奋 в LIMIN 1 K A., в  $W_{1}$ D. 0|0|PPO N O 0 P i G K. P Q 62 OR X | X | WK L M N G. 0 WWXY. IIKLMNOPO G. - HI XXX IK. M M01 0 YYZABC HIJKLMNOP D. WX E. G. 0. R. SIT ZZABCDEFGHIJKLMNOPORSTUVWXY

Vigenere Table

#### Route Cipher

• Belongs to Transposition Family

• Lots of Possible Keys

#### Route Cipher

• Plaintext: attack at dawn. hello world.

• Key: Descending Vertical Column.

• Ciphertext: akwll tanod tthwq adeoq calrq

	1	2	3	4	5		
1	а	k	w	ł	I		
2	t	а	n	0	d		
3	t	t	h	W	q		
3	а	d	е	0	q		
5	с	а	I,	r	q		

## VIC Cipher

• Belongs to Nihilist Ciphers

• Used by PoWs in Vietnam

• Regarded as Most Complex Hand Cipher



• Checkerboard Transposition

## VIC Cipher

• Plaintext: Attack at dawn

• Ciphertext: 03-01-01-03-21-27 03-01 22-03-65-05

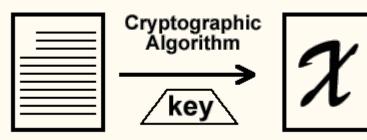
	0	1	2	3	4	5	6	7	8	9
	E	T		А	0	N		R	0	S
2	В	C	D	F	G	Н	J	K	L	М
6	Ρ	Q	1	U	V	W	Х	Y	Ζ	

Straddling Checkerboard

• Terms

• History of Selected Ciphers

• Example Ciphers



plaintext

ciphertext

	A	8	¢	D	ε	,	G	н	1	1	К	L.	м	N	0	P	0	R	5	τ	U	٧	W	х	Y	z
٨	A	в	c	D	Ε	F	G	н	1	1	К	L	н	N	0	P	Q	R	5	т	U	γ	W	х	Y	Z
в	8	C	D	E	F	G	H	1	1	ĸ	L	M	N	0	P	0	R	s	т	U	V	W	x	Y	z	A
Ċ	C	D	Е	F	G	н	1	1	ĸ	L	м	N	0	Ρ	0	R	5	т	U	٧	W	х	Y	z	A	в
D	D	E	F	G	н	1	1	ĸ	L	М	N	0	P	Q	R	5	Т	U	۷	W	х	Y	z	A	в	C
E	E	F	G	H	1	1	K	L	М	N	0	ρ	Q	R	s	Т	U	٧	W	х	Y	z	A	В	с	D
F	F	G	H	T	1	ĸ	E	м	N	0	p	0	R	5	T	U	v	W	х	Y	z	A	8	¢	D	ε
Ġ	G	н	1	1	ĸ	L	м	N	0	p	0	R.	5	т	U	v	w	х	Y	z	A	8	c	D	E	۲
н	H	1	1	ĸ	L	м	N	0	P	0	R	5	т	U	٧	W	x	Y	z	٨	8	C	D	E	F	G
1	1	1	ĸ	L	м	N	0	P	0	R	s	т	U	٧	w	х	Y	z	A	в	C	D	Е	F.	G	н
ſ	T	ĸ	L	М	N	0	P	Q	R	5	Т	U	۷	W	х	Y	z	A	в	C	D	E	F	G	н	1
ĸ	K	L	м	N	0	Ρ	Q	R	s	Т	υ	v	W	х	Y	z	A	в	С	D	ε	F	G	H	1	J
Ľ	L	M	N	ō	P	Q	R	5	T	υ	V	W	×	Y	Z	A	в	C	D	Ε	F	G	H	1	J	K
М	м	N	0	р	0	R.	5	Т	U	v	W	x	Y	z	A	8	C	D	ε	۴	G	н	1	J.	ĸ	L
N	N	0	P	0	R	5	τ	U	v	W	X	Y	z	A	8	C	D	E	F	G	н	1	1	ĸ	L	М
0	0	Ρ	0	R	5	τ	U	٧	W	х	γ	z	٨	8	C	D	E	F	G	н	1	J	ĸ	L	М	Ν
Ρ	P	0	R	5	т	U	٧	W	X	Y	z	A	в	C	D	E	F	G	н	1	1	Ŕ	L	М	N	0
Q	9	R	5	Т	U	٧	W	х	Y	z	A	в	C	D	E	F	G	н	1	1	ĸ	L	м	N	0	Ρ
R,	R	5	Т	U	٧	W	x	Y	Z	A	B	C	D	ε	F	G	H	1	J	ĸ	£.	M	N	0	ρ	Q
ŝ	5	т	U	٧	Ŵ	х	Y	z	A	В	¢	D	٤	F	G	н	1	1	ĸ	L	М	N	0	P	Q	R,
٣	Ť	U	v	W	x	¥	z	A	8	Ċ	D	6	+	G	н	1	1	ĸ	L.	н	'N	0	P	Q	R	5
Ü	U	γ	W	х	Y	z	A	8	C	D	Ε	F	G	н	1	1	8	L	м	N	0	P	0	R	5	τ
٧	٧	W	х	Y	Z	A	в	C	D	E	F	G	н	1	1	ĸ	L	м	N	0	P	0	R	5	т	U
									E																	
х	X	Ŷ	Z	A,	в	C	D	E	F	G	н	1	j.	K	L	М	N	0	Ρ	Q	R	5	T	U	٧	W
									G																	
									н																	