

Breaking the Vigenère Cipher

Introduction

Vigenère Cipher

Message Meet Me At Dawn

Key

- Previously: learned Caesar cipher
- Now: Vigenère cipher

Vigenère Cipher

Message Meet Me At Dawn

Key DICE

- Previously: learned Caesar cipher
- Now: Vigenère cipher
 - Key is "word" (array of ints)

Vigenère Cipher

Message Meet Me At Dawn

Key D I C E D I C E D I C E D I C

- Previously: learned Caesar cipher
- Now: Vigenère cipher
 - Key is "word" (array of ints)

Vigenère Cipher

Message Meet Me At Dawn

Key 3 8 2 4 3 8 2 4 3 8 2 4 3 8 2

- Previously: learned Caesar cipher
- Now: Vigenère cipher
 - Key is "word" (array of ints)

Vigenère Cipher

Message Meet Me At Dawn

Key + 382438243824382

Encrypted

- Previously: learned Caesar cipher
- Now: Vigenère cipher
 - Key is "word" (array of ints)

Vigenère Cipher

Message	Meet Me At Dawn
Key +	382438243824382
Encrypted	

- Previously: learned Caesar cipher
- Now: Vigenère cipher
 - Key is "word" (array of ints)

Vigenère Cipher

Message	Meet Me At Dawn
Key +	382438243824382
Encrypted	P

- Previously: learned Caesar cipher
- Now: Vigenère cipher
 - Key is "word" (array of ints)

Vigenère Cipher

Message	M	e	e	t		M	e		A	t		D	a	w	n
Key +	3	8	2	4	3	8	2	4	3	8	2	4	3	8	2
Encrypted	P														

- Previously: learned Caesar cipher
- Now: Vigenère cipher
 - Key is "word" (array of ints)

Vigenère Cipher

Message	Me	e	t		M	e		A	t		D	a	w	n	
Key +	3	8	2	4	3	8	2	4	3	8	2	4	3	8	2
Encrypted	P	m													

- Previously: learned Caesar cipher
- Now: Vigenère cipher
 - Key is "word" (array of ints)

Vigenère Cipher

Message Meet Me At Dawn

Key + 382438243824382

Encrypted Pmgx Ug Db Hdep

- Previously: learned Caesar cipher
- Now: Vigenère cipher
 - Key is "word" (array of ints)

Vigenère Cipher

Message Meet Me At Dawn

Key + 3 8 2 4 3 8 2 4 3 8 2 4 3 8 2

Encrypted Pmgx Ug Db Hdep

- Conceptually: multiple Caesar ciphers
 - Can re-use code: Array of CaesarCipher
 - Use "mod" to wrap around 0,1,2,3,0,1,...

Vigenère Cipher

Message M e e t M e A t D a w n

Key + 3 8 2 4 3 8 2 4 3 8 2 4 3 8 2

Encrypted P m g x U g D b H d e p

- Mini-Project:
 - We provide VigenereCipher code
 - You write cracker—break the cipher