Breaking the Vigenère Cipher

Introduction

Duke
UNIVERSITY

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 `DICEDICEDICEDIC`

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

Vigenère Cipher

Message `Meet Me At Dawn`

Key `3824382438243 82`

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

Vigenère Cipher

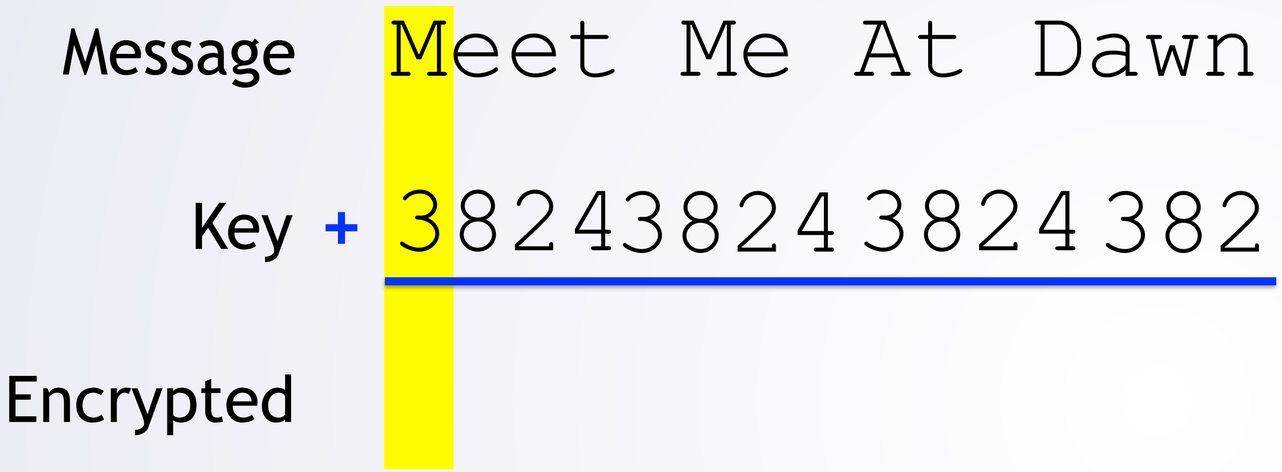
Message `Meet Me At Dawn`

Key + `3824382438243 82`

Encrypted

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

Vigenère Cipher



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

Vigenère Cipher

Message	Meet Me At Dawn
Key +	3824382438243 82
Encrypted	P

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

Vigenère Cipher

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

Vigenère Cipher

Message	Meet Me At Dawn
Key +	3824382438243 82
Encrypted	Pm

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

Vigenère Cipher

Message	`Meet Me At Dawn`
Key +	`3824382438243 82`
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 +	3824382438243824
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	Meet Me At Dawn
Key +	3824382438243824
Encrypted	Pmgx Ug Db Hdep

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