MATH 314 Spring 2018 - Class Notes

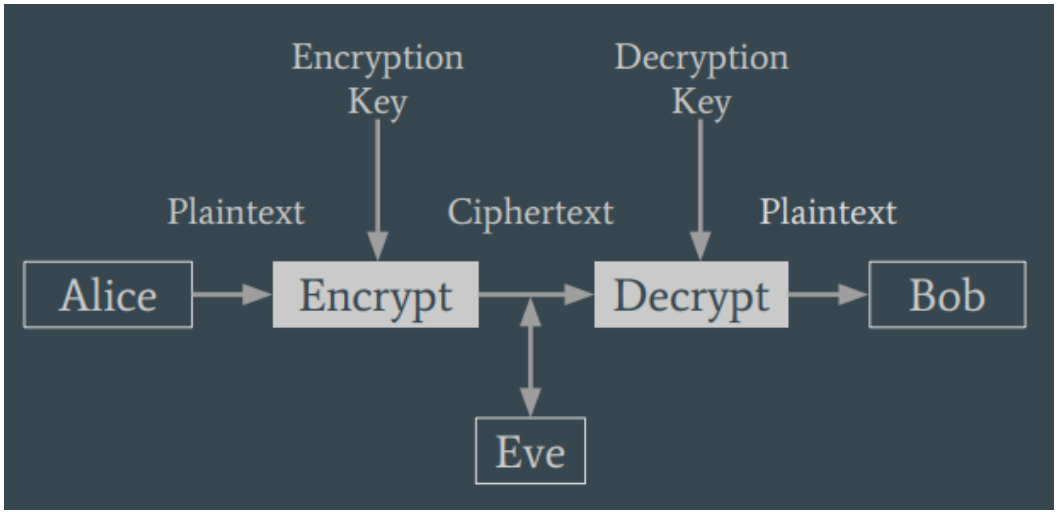
1/30/2018

Scribe: Rachael Clayton

Summary: Today's class covered a brief history of cryptography and an introduction to early ciphers and how they work.

Notes:

- The word cryptography is derived from a combination of two Greek words meaning "hidden, secret", and "writing".
- Cryptography is the writing (or designing systems to write) messages secretly, while cryptanalysis is the study of methods to analyze and break hidden messages.
- We then introduces a scenario introducing Alice, Bob, and Eve.



  - Symmetric Key: Alice and Bob use a (pre-shared) secret key.
  - Public Key: Bob makes an encryption key public that Alice uses to encrypt a message. Only Bob has the decryption key.

Possible attacks: Eve, the eavesdropper, is trying to:

  - read Alice's message
  - tamper with Alice's message so that Bob receives an altered message
  - find Alice's to read all of Alice's messages
  - pretend to be Alice and communicate with Bob

Why does this matter?

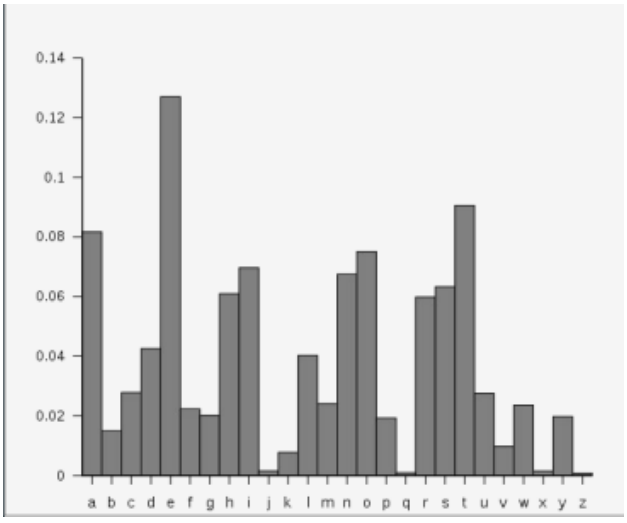
- Confidentiality
  - Only Bob should be able to read Alices message.
- Data integrity
  - Alices message shouldnt be altered in any way.
- Authentication
  - Bob wants to make sure Alice actually sent the message.
- Non-repudiation
  - Alice cannot claim she didnt send the message.

Caesar Cipher

- Messages were encrypted by shifting the alphabet a certain number of letters.
- Example: "Et tu, Brute?" shifted 3 letters
  - Plaintext: `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`
  - Ciphertext: `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`
  - Plaintext: `ET TU BRUTE`
  - Ciphertext: `HW WX EUXWH`

9th and 10th century

- Arabs invented cryptanalysis, systematic study of ways of deciphering a code without a key.
- Frequency Analysis: Comparing how frequently letters occur to decipher the code.

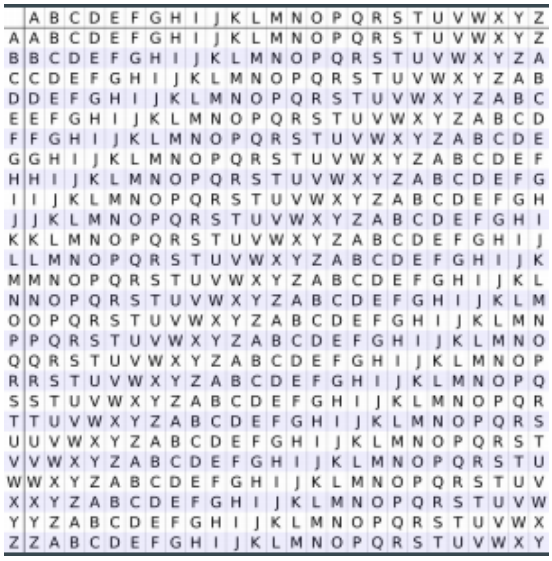


15th century

– Nulls and added characters are implemented to confuse potential enemies
– Evidence in the Babington Plot to assassinate Queen Elizabeth, resulting in the trial and execution of Mary, Queen of Scots

1586 - The Vigenère Cipher

– Blaise de Vigenre reinvents Giovan Battista Bellasos cipher.
– One letter is no longer encoded the same way every time.
– Described as unbreakable by many, including Lewis Carroll.
– Example: Encrypting Attack at dawn using LEMON

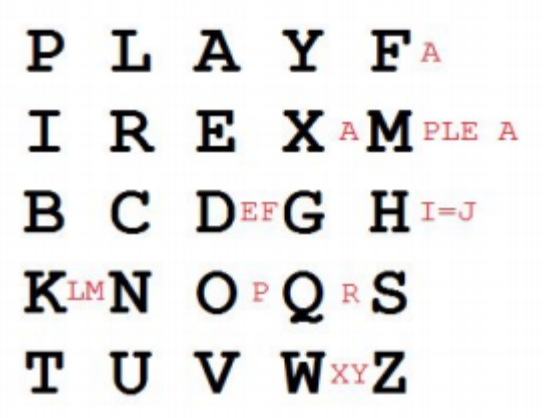


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

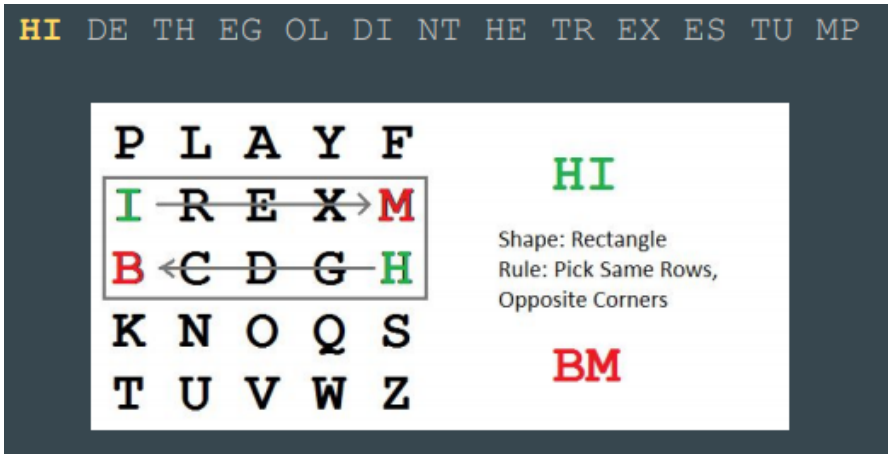
  * Plaintext: `ATTACKATDAWN`
  * Key: `LEMONLEMONLE`
  * Ciphertext: `LXFOPVEFRNHR`

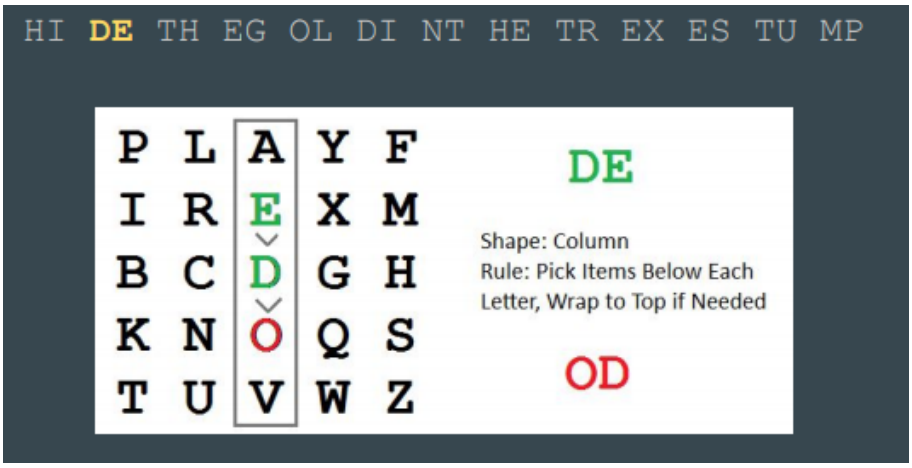
1854

  * Charles Babbage found a solution to the Vigenère cipher.
    · Analytical Engine
    · "Father of the Computer" along with Ada Lovelace
  * Playfair cipher invented by Sir Charles Wheatstone (but named after the Baron Playfair)
    · Encrypts pairs of letters instead of single letters, so frequency analysis isnt as useful to break the cipher
    · Used by the British in WWI.
    · Uses a 5x5 table with a keyword or phrase
  * "Playfair" Example:



· Encrypt "Hide the gold in the tree stump"
· HI DE TH EG OL DI NT HE TR EX ES TU MP
· the X separates the two E's, because they are repeated characters





HI DE TH EG OL DI NT HE TR EX ES TU MP
BM OD ZB XD NA BE KU DM UI XM MO UV IF
Decryption requires working backwards

The 1920s-1940s

- Enigma machines (Germany)
- Most notably used in WWII
- Polish Cipher Bureau started breaking Enigma messages.
- Alan Turing later improved the Polish methods.
- Called Bombes

The Encryption Function and Modular Arithmetic

- If we look at the Caesar Cipher closely, we can change the letters into numbers
- A - 0
- B - 1
- .
- .
- .
- Z - 25
- The Key, k, is the shift amount
- **Encryption function:**
  - $E(x) \equiv x + k$
- Example: Encrypt BAT using k = 7
  - $E(x) \equiv x + k$
  - B - 1, A - 0, T - 20
  - $E(1) \equiv 1 + 7$
  - $E(1) \equiv 8$ - "I"

* $E(0) \equiv 0 + 7$
* $E(0) \equiv 7$ - "H"
* $E(20) \equiv 20 + 7$
* $E(20) \equiv 27$ - what do we do when the number is greater than 26?
* This is where we implement modular arithmetic
    - Because we can't exceed 26, we need to be able to "wrap around"
    - In other words, we can divide by 26 and take the remainder.
* The notation for modular arithmetic is this:
    - $E(x) \equiv x + k \pmod{26}$
    - The equivalence symbol is represented by 3 parallel lines.
    - $a \equiv b \pmod{m}$ if b is the remainder when you divide a by m
* So, $E(20) \equiv 20 + 7 \pmod{26}$. $E(20) \equiv 27 \equiv 1 \pmod{26}$ - B
* BAT is encrypted to IHB
* Since we can reduce equations modulo 26 before computing, there are really only 26 different values for k
* $0 <= k <= 25$