INTRODUCTION TO CRYPTOGRAPHY

DR. O. I. ADELAIYE

WHAT IS CRYPTOGRAPHY?

- Is a Greek word
  - *κρυπτο* (crypto), secret
  - *γραφη* (graphy), writing
- ”The art of mangling information into apparent unintelligibility in a manner allowing a secret method of unmangling”
- Allows the transformation of a plaintext (cleartext) into a ciphertext and vice versa

  Plaintext ciphertext = encryption

  Ciphertext plaintext = decryption

WHY CRYPTOGRAPHY?

- Protects stored data
- Protects data in transit
- Provides protection against
  - Data eavesdropping
  - Tampering with data
- Could be easily used for authentication purposes

ANY TERMINOLOGY AT ALL?

- Suuuuuuuuuuuure !
- Cryptography
  - art of creating and using codes to secure transmission of information
- Cryptanalysis
  - art of obtaining original message from ciphertext without access to secret information (key or algorithm itself)
- Cryptology
  - combines cryptography and cryptanalysis

WHEN DID IT ALL START?

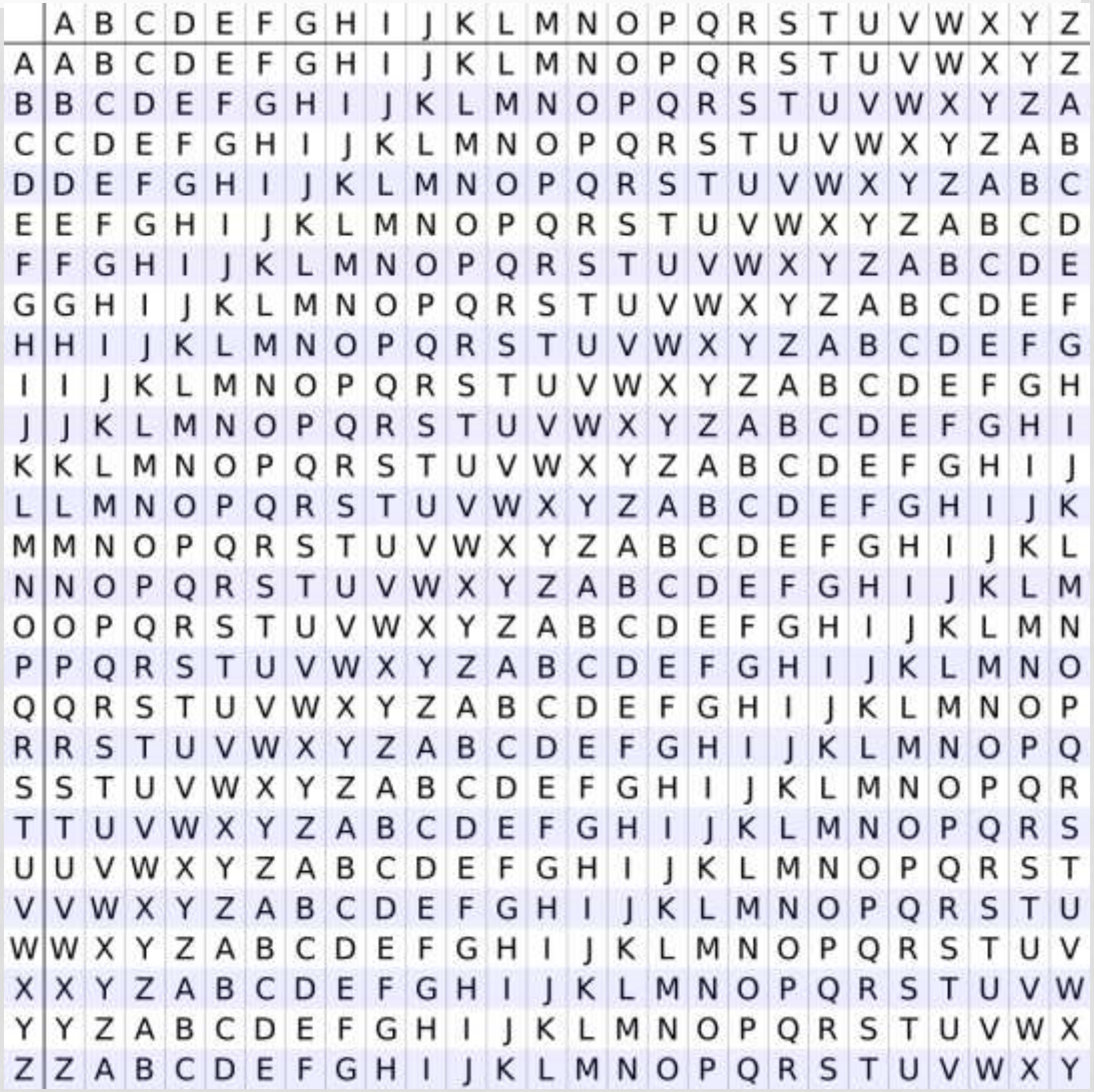
- Julius Caesar (sometime BC) !
  - A substitution cipher
  - The Caesar cipher replaces the *ith* letter by the *i+3th* letter
    - CAT becomes FDW
    - Wraps around to A from Z
- Generalised in monoalphabetic ciphers
  - No restriction (such as *i* □*i*+3) on which letter could be assigned to which
    - E.g. A is encrypted as B, B as D, C as Z, D as A, etc.
    - 26! possible monoalphabetic ciphers (4x1026)
  - Stronger than Julius Caesar, but would you use it?
    - NO ! Vulnerable to statistical analysis
  - Most common English letters?

WHAT HAPPENED NEXT?

- Vigenere Cipher
  - Not his
  - First appeared in Rome in “La cifra del. Sig. Giovan Battista Bellaso”, in 1553
  - “Le chiffre indéchiffrable” for about 3 centuries
  - Similar to a Caesar cipher but has a variable shift value
    - First letter shifted by 5, second by 17, third by 11
    - 5, 17 and 11 are defined by a secret
    - The values range is 0 to 25 (A to Z): A is 0, Z is 25

WHAT HAPPENED NEXT?

- Vigenere Cipher
  - If the message to be encrypted is longer than the key, then the key is repeated
- Example: Encrypt **H**ACKNOW using CAT
  - Repeat key to match message's length
    - CATCATC
  - The table shows how to encrypt
  - **H** row, C column = encrypted H = ?
- Decipher by going to row C and look for "?" inside the row (not in the column index), the corresponding column index is the cleartext



	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

BREAKING A CRYPTOGRAPHIC ALGORITHM

SHOULD CRYPTO. ALGORITHMS BE KEPT SECRET?

- Keeping an algorithm secret prevents crackers from knowing it they cannot break it
  - Security through obscurity
- Difficult in practice
  - Each time you use the algorithm with someone, they need to learn it (and might leak it?)
  - If it is implemented in some hardware, reverse-engineering it could reveal the algorithm

SHOULD CRYPTO. ALGORITHMS BE KEPT SECRET?

- Making an algorithm available makes it possible for crackers to do all tests on the algorithm
  - And all the good guys too
  - Asa a good guy finds a loophole, she warns people
- Fundamental Tenet of Cryptography
  - "If lots of smart people failed to solve a problem, then it probably won't be solved (soon)"
- Nowadays, most of commercial algorithms are public, whereas some military algorithms are kept secret

SHOULD CRYPTO. ALGORITHMS BE KEPT SECRET?

- Kirchhoff's principle
  - A cryptographic algorithm must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience
  - Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents
- The only secret in the system should be the key

HOW DIFFICULT IS IT TO FIND A KEY?

- Assume you are using an algorithm with a 16 bit key
  - 2^{16} (=16384) possible keys
  - If a computer can test 100 keys/sec, then it will take a bit less than 3 minutes to try all of them
    - brute-force
  - And, in average, half that time to find the right key
  - This time doubles for each added bit (0 or 1)
  - For a 24 bit key, the same computer will need almost 20 months to try all combinations
- In practice, computers are much faster, but keys are much longer too !
- We would say that it is computationally infeasible to brute-force a cryptographic algorithm if it required an unreasonable amount of time using the most powerful computers

HOW DIFFICULT IS IT TO FIND A KEY?

- Note that if the keys are chosen and used by humans, then they have limited choices
  - 24 bit key is a 3 character key
  - Say for example that the used characters are upper and lower case and numerals
  - 26+26+10 = 62 possibilities for each character
  - 62^3(=238328) possible keys in all
  - Takes less than an hour to try all combinations !
- Nowadays, 280 possible combinations are considered feasible

HOW TO BREAK A CRYPTO ALGORITHM?

- Three typical attacks
  1. Ciphertext only
     - Attacker has access to encrypted messages
     - The attacker has to try possible keys in turn until one works
     - The attacker has to be able to recognize that a key actually works
       - Hence the name recognizable plaintext attack
     - Problem when dealing with a cipher text that can be decrypted in several ways
       - Should have many samples
       - Does not occur with modern crypto algorithms (too randomised outputs)

HOW TO BREAK A CRYPTO ALGORITHM?

- Three typical attacks

  2. Known Plaintext
     - The attacker obtained pairs of plain and cipher texts
     - Could be because the meaning of the ciphertext was revealed
       - Attack? Yes, no
       - Next target?
     - Should prevent attackers from getting those pairs
       - Adding a sequence number

HOW TO BREAK A CRYPTO ALGORITHM?

- Three typical attacks

  3.Chosen Plaintext

  - The attacker can choose the plaintext and make the system encrypt it !
  - Real life example: WEP
    - In WEP, the access point can send random numbers to the station (e.g. laptop) and the station encrypts and returns it
    - An attacker could pretend to be the access point
  - Same if there are only few possible meanings of the ciphertext
    - E.g. YES or NO

TYPES OF CRYPTOGRAPHIC ALGORITHMS

DO ALL CRYPTO ALGORITHMS WORK THE SAME WAY?

- Three types of crypto algorithms
  1. Secret key algorithms
     - Most intuitive: same key for encryption and decryption
     - Also known as Symmetric Cryptography
     - Many uses in secure systems, one of the most obvious ones is confidentiality
     - The two communication parties have to find a way of sharing the key before communicating
       - More on this later

DO ALL CRYPTO ALGORITHMS WORK THE SAME WAY?

- Three types of crypto algorithms

  2. Public key algorithms

     - Keys work in pairs
     - When a key is used to encrypt, only the other one can decrypt
       - Can encrypt with either; different uses
     - Also known as Asymmetric Cryptography
     - Typically one key is kept secret (private key), the other one is made public (public key)
     - Many uses in secure systems, one of the most obvious ones is authentication
     - The two communication parties have to find a way of sharing public key(s?) before communicating
       - More on this later

DO ALL CRYPTO ALGORITHMS WORK THE SAME WAY?

- Three types of crypto algorithms

  3.Hash algorithms

  - A one-way transformation
    - If *h* is a hash function such that *y=(h)*, then it is **computationally infeasible** for a user who has *h* and *y* to find x(or an x' ?such that *h(x')*=y)
  - Gives a fixed length output, whatever the input size is
    - MD5's is 128, SHA-1's is 160
  - The output is sometimes called hash, digest or checksum
  - Many uses in secure systems, one of the most common ones is digital signatures
    - More on this later

EN

D