Cryptography

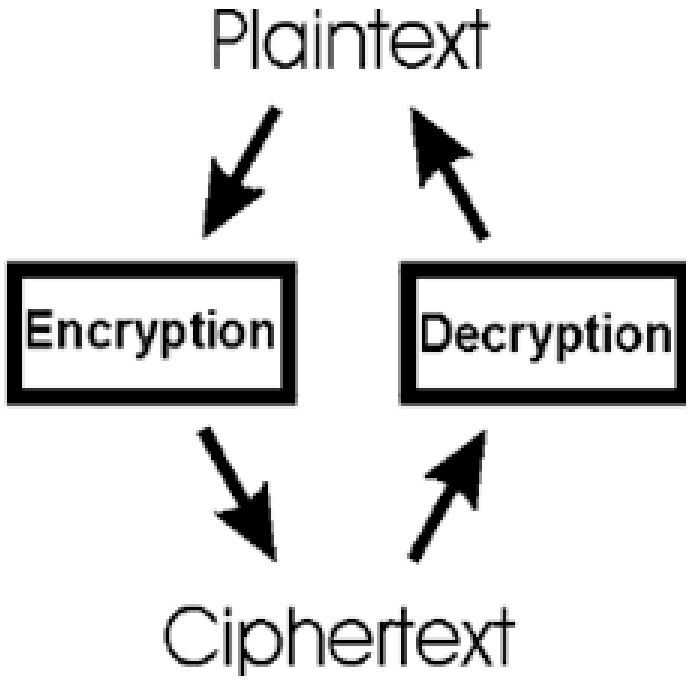
Neal Mazur

Cryptography

- Definition: the art of solving codes
- In computer science: Cryptography, or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

Cryptography

- Encryption: The method by which information is converted into secret code that hides the information's true meaning.
- Decryption: the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.



Need for Cryptography in Computer Science

- Password Protection
  - Security of Individual Accounts
    - Passwords for Banking, Purchasing, Network Access, Utilities, Payroll, etc.
    - How secure is my password: https://howsecureismypassword.net/
  - Security of Company Password Files

Computer Password Hacking Techniques

- Brute Force
- Dictionary Attack
- Masking
- Guessing
- Shoulder Surfing

Computer Password Hacking Techniques

- Brute Force
  - Try every combination of characters
  - Defense: Lengthy passwords with large set of characters
  - Assuming 1,000,000,000,000 passwords tried each second

Password Length	Size of Set	Combinations	Time to Crack
3	26	3^{26}	2 seconds
10	62	10^{62}	10^{50} years

Other Cryptographic Hacking Techniques

- Dictionary attack: Commonly used words, and phrases are tried
- Masking: Brute force with restrictions (start with an uppercase letter)
- Guessing: Standard passwords, hobbies, pets, family names, date of birth, etc.

Secure Passwords at a Company

- A company must store all user passwords in a database
- Clear Text:

User Name	Password
NealMazur	Gr8tpaSs)(werd
BettyBoop	mypassword

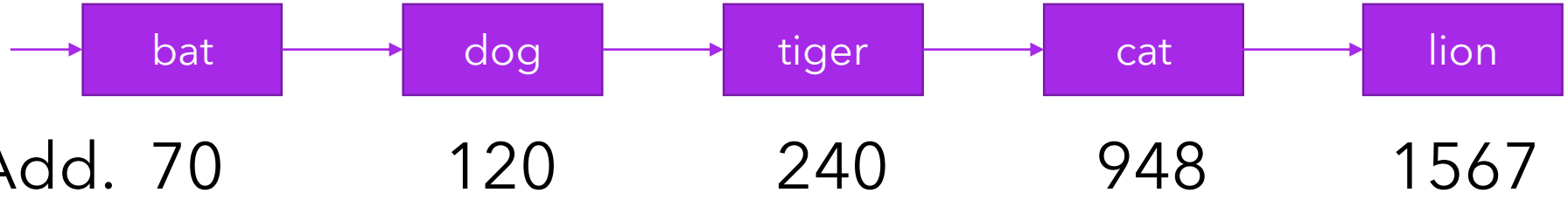
- What's the problem?

Hashing

- Hashing encodes text (or other information) into a fixed size hash value
- A hash function is used to make this translation:
  - hash (word) -> product of ASCII values of the characters mod 1000
  - cat = 99 x 97 x 116 % 1000 = 1,113,948 % 1000 = 948

Hashing

- cat = 99 x 97 x 116 % 1000 = 1,113,948 % 1000 = 948
- Can be used for quick retrieval from a database:



- Instead of linear/binary search, we access the data immediately through the hashed address

Hashing Passwords

- A hash function is:
  - Repeatable
  - One way
- Password Database now looks like this:

User Name	[redacted]	Hash (Password)
NealMazur		83ksl329fa939kf%43/293
BettyBoop		9382+3*3928402!39310l

Cryptography on the Internet

- Information is passed across the internet using binary (1's and 0's)
- Code.org Video: https://www.youtube.com/watch?v=ZhEf7e4kopM
- So we can represent numbers, characters, images, sounds, video across the internet

Information Sending

- There are a number of ways of “encrypting” this information as 1’s and 0’s:
  - Text (ASCII, EBCDIC)
  - Image (JPG, GIF, PNG,…)
  - Sound (MP3, WAV, …)
- Both sender and receiver have to agree on the particular representation of the information
- Bits look like bits, without agreement on the type of representation, communication cannot take place

BUFFALO STATE
The State University of New York

Google CS[4]HS

Cybersecurity Lesson Plan Teams

Team A	Mariel	Schneggenburger	Orlando	Buria
Team B	Robert	Uldrich	Marcy	Boyd
Team C	Bryan	Hansen	Denise	Seibert
Team D	Janelle	Harb	Mike	Lieber
Team E	Kaci	Nowadly	Andrea	Morganti
Team F	David	Lasky	Clyvette	Grayson
Team G	Graham	Hayes	Kevin	Gee
Team H	David	Czechowski	Mary Jo	Andalora
Team I	Alexandria	Porter	James	Campbell
Team J	Morgan	Popple	Kristin	Holmes
Team K	Patricia	Wojtowicz	Christine	Owens
Team L	Sedat	Yalcin		

Zoom Internet

- What is the Internet? https://www.youtube.com/watch?v=Dxcc6ycZ73M
- We will use Zoom's chat feature to represent the internet
- Make sure we all have a partner
- Send a single word text message to your partner
  - Did you get it?
  - Can you steal one?

Zoom Internet

- Look up an ASCII table
- Send a single word text message to your partner in base 10 ASCII
  - Did you get it?
  - Can you steal one?
- Encryption and Public Keys: https://www.youtube.com/watch?v=ZghMPWGXexs

Caesar Cipher

- We would like to encrypt our message so it is not as easy to steal
- A Caesar Cipher offsets each letter in a message by a certain number of letters in the alphabet
- A "key" tells the number of letters to shift
- To encrypt if the key is 4, we have:

a → e, b → f, c → g, … y → c, z → d

- bat → fex
- What is the decrypt key?
- Programming the Caesar Cipher in Python: https://projects.raspberrypi.org/en/projects/secret-messages

Python problem

- Compute the cube of 17 divided by 5
- Print the result
- Find the position of ‘u’ in the word intellectual
- Print the position

Sending the Caesar Cipher Message

- Let’s set our key to 1
- Send a single word message to your partner
  - Did you get it?
  - Can you steal one?
- Send a private message to your partner with the key
- Send a single word message to your partner
  - Did you get it?
  - Can you steal one?

Vigenère Cipher

- Variation of the Caesar Cipher
- The Caesar Cipher shift distance changes each letter based on key word
- An alphabetical grid is used to apply the key to encrypt/decrypt the letters
- Code.org Widget for Vigenere Cipher:

https://studio.code.org/s/vigenere/stage/1/puzzle/1

Vigenère > Caesar

- Drawback of Caesar
  - Limited number of keys
  - Natural language letter frequency
- Vigenère
  - Many keys
  - Letter frequency not easily determine
  - Can be broken, helps to know the length of the key

Enigma Machine

- World War II Nazi Code Machine
- In a sense similar to the Vigenere code in that the encryption changes with each character sent
- A difference is that a physical machine is being used to change the translation as opposed to a letter of text
- Here is a video that gives an example of its use:

https://www.youtube.com/watch?v=-mdSvGUd0_c

Bacon's Cipher

- **Steganography** is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.
- We will demonstrate this idea using a Bacon Cipher
- In this example, we will use ASCII and 1's and 0's. The actual Bacon encoding is different (actually two codes) and A's and B's are used but we will simplify with what we know
- Two type faces are used. Let's say bold represents 1 and plain text represents 0.
- **H**ell**o J**im ➔ 01001100 ➔ L
- The actual text is ignored

Bacon's Cipher

- Translate:

C**o**uld s**om**e**on**e **g**ive m**e a** b**ig cu**t**tin**g board?

- Answer:

01000011 01101000 01101111 01110000

C h o p

Encryption on the Internet

- **Symmetric-key** algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.
- In a sense, similar to the Vigenere encryption where after each character is translated, the key changes for the next.
- The key is very long so it does not repeat often.
- 128 – 256 bits used
- $2^{128} = 10^{77}$
- Brute Force attempt is not feasible but if the key is stolen!

Encryption on the Internet

- **Asymmetric Encryption** is a form of encryption where keys come in pairs. What one key encrypts, only the other can decrypt.
- A **public key** (available to everyone) is what is used to encrypt the information
- A **private key** (known only to the receiving site) is used to decrypt the information
- An intercepted message cannot be decoded without the private key

Asymmetric Key Encryption/Decryption Math!

- The RSA (Rivest–Shamir–Adleman) algorithm, published in 1977, describes a process commonly used for asymmetric encryption
- An example to follow
- Two keys must be generated:
  - Public Key
  - Private Key

Generating the Public Key

- Choose two very large (say 500 digits) prime numbers (secretly)
- For our example (to do the math) we will choose prime numbers:

  $p = 5, q = 11$

- Compute their product which we will call modulus:

  $modulus = p \times q = 55$

Generating the Public Key

- Choose two very large (say 500 digits) prime numbers (secretly)
- For our example (to do the math) we will choose prime numbers:

  $p = 5, q = 11$

- Compute their product which we will call modulus:

  $modulus = p \times q = 55$

Generating the Public Key

p = 5, q = 11, modulus = 55

- Compute product:

product = (p – 1) x (q – 1) = 40

- Select a number that is relatively prime to 40 (no common factors other than 1) which is also less than 40. 10 would not work for example. Let's choose 7. Call this e_public.
- We have our public key: (e_public, modulus) = (7, 55)

Generating the Private Key

p = 5, q = 11, modulus = 55, product = 40, e_public = 7

- Find a number, e_private such that:

(e_private x e_public) mod product = 1

(e_private x 7) mod 40 = 1; e_private = 23

(23 x 7) mod 40 = 161 mod 40 = 1

- Wolfram Alpha is a computational knowledge engine or answer engine developed by Wolfram|Alpha LLC, a subsidiary of Wolfram Research.

Keys Generated

p = 5, q = 11, modulus = 55, product = 40, e_public = 7

e_private = 23

- So we have:

public key = (e_public, modulus) = (7, 55)

private key = (e_private, modulus) = (23, 55)

- public key encrypts; private key needed to decrypt

Encrypting using Public Key

p = 5, q = 11, modulus = 55, product = 40, e_public = 7

e_private = 23

- Assume a data value of: data = 2
- ciphertext = $data^{e\_public}$ mod modulus

2^7 mod 55 = 128 mod 55 = 18

ciphertext = 18

- Can we just reverse this process?
  - unfeasible for large values

Decrypting using Private Key

p = 5, q = 11, modulus = 55, product = 40, e_public = 7

e_private = 23, plain text = 2, ciphertext = 18

- plain text = $\text{ciphertext}^{\text{e\_private}}$ mod modulus

plain text = 18^{23} mod 55

plain text = 743477136140219279133187768 32 mod 55

plain text = 2

Notes on Asymmetric Cryptography

- The following process was used for public key encryption:
- ciphertext = $data^{e\_public}$ mod modulus

  2^7 mod 55 = 128 mod 55 = 18

  - Can we just reverse this process using just the public key?
    - unfeasible for large key values typically used in encryption
- Asymmetric cryptography can be very expensive. Symmetric encryption is often used with the only use of Asymmetric encryption being the transfer of keys
- Can we use letter frequency in a message with text?
  - Grouped characters are often encrypted so that this information is hidden