BLOWN TO BITS: CHAPTER 5

Paul B., Dennyse B., Izavelle M., Jason P., Cassy S.

Jason Pgs. 4-10

- In the wake of the 9/11 attack, Senator Judd Gregg proposed a legislative plan to have keys for encryption in escrow under the U.S Government
- The use of the Internet for commercial use created a paradox for the U.S, where people around the world required safe, strong encryption, but needed to limit, or be able to decrypt messages of terrorists or criminals.
- Encryption shifted from use of Governments and heads of state to something that is required by the public to protect their sensitive data on the internet
- Encryption & Decryption: Encryption is the encoding of data to create a secure message. Decryption is the conversion of encrypted data to it's unencrypted form.
- Cryptography: "Secret writing", the art of writing or solving codes

Cassy Pgs. 11-17

- Frequency analysis: a technique used to crack codes if the code is a basic substitution cipher
- Substitution Cipher: a code where letters have a corresponding symbol to represent them
- Vigenère Cipher: a technique that uses multiple **Caesar Ciphers** (letter shifted up or down the alphabet) at various parts of the code
- Vigenère Ciphers can be broken with the use of the One-time-pad, an algorithm that combines plaintext with a random key,
  - Keys come together in a pad of paper and each key can only be used once before discarding and destroying
- One time pads are the **only** mathematically unbreakable encryption to exist
- One-time-pads are not used because they are not practical

Dennyse Pgs. 18-24

- A secure encryption algorithm is one of the “holy grails” of Computer Science
- Mathematical certainty would not suffice to create perfect security if people don’t change their behavior

- Rather than creating a cryptographic method to be SECRET, it’s better to create one to be SECURE
- Protecting keys was a military and diplomatic priority of supreme importance
  - Only gov. had the money & means to assure production, protection, distribution of keys which depends on secret communication
- Find a means of encrypting the message so that the ciphertext reveals no patterns from which the key could be inferred
- **THE KEY AGREEMENT PROTOCOL**: One way computation with 2 important properties
  - Can be DONE quickly, cannot be UNDONE quickly

Paul Pgs. 25-30

- Public key Encryption is a form of the Key agreement protocol but in a slightly different order
- it allows anyone to encrypt a message but only lets a specific person decrypt it which helps people communicate through insecure places
- Digital signatures are made from *message digests* and help verify the legitimacy of the encrypted message.
- Nowadays one way computations are used everywhere such as in a websites that deal with encrypted web transactions.

Izavelle Pgs. 31-36

- Internet use became apparent:
    - People would want privacy on their internet/communication and intelligence agencies became scared because they feared it would interfere with their most powerful tool “wiretapping”
- Late 1980’s-early 1990’s: Cryptographic Systems
    - Cryptographic products could not be exported w/out a license violating export controls resulted in severe criminal penalties
    - people everywhere needed easy-to-use, cheap, uncrackable cryptography that could communicate without governments being able to understand them.
- Crypto Wars
    - Remainder of the 1990s. Law enforcement and national security argued the need for encryption controls.

Izavelle Pgs. 31-36

- Zimmermann (Journeyman programmer and civil libertarian who was interested in cryptography)
    - Zimmermann set about to produce encryption software for the people, to counter the threat of increased government surveillance.
    - June of 1991: completed a working version of his software; “Pretty Good Privacy.” (Appeared on many computers around the U.S.
        - Made the government upset (caused criminal investigation)
- International ECHELON System
    - “eavesdropping enterprise“
    - Encrypted communication goes many ways

REFLECTION/QUESTIONS

1. Why wouldn’t more people use One-time-pads if they’re the only mathematically unbreakable encryption to exist? Even with all of the hassle it is to use it, wouldn’t it be worth it?
2. Why won’t people change their online habits & behavior if they acknowledge their online security is at risk?
    a. If accessibility to better technology is the cause of the issue, how do we make technological inventions more accessible to everyone?
3. How has the use of cryptography change the way we interact online and how different would it be in the future as technology advances?
4. Can anybody get the information they want if involved with International ECHELON System? Or can it only do so much (limitations)?