Communicating in Secret

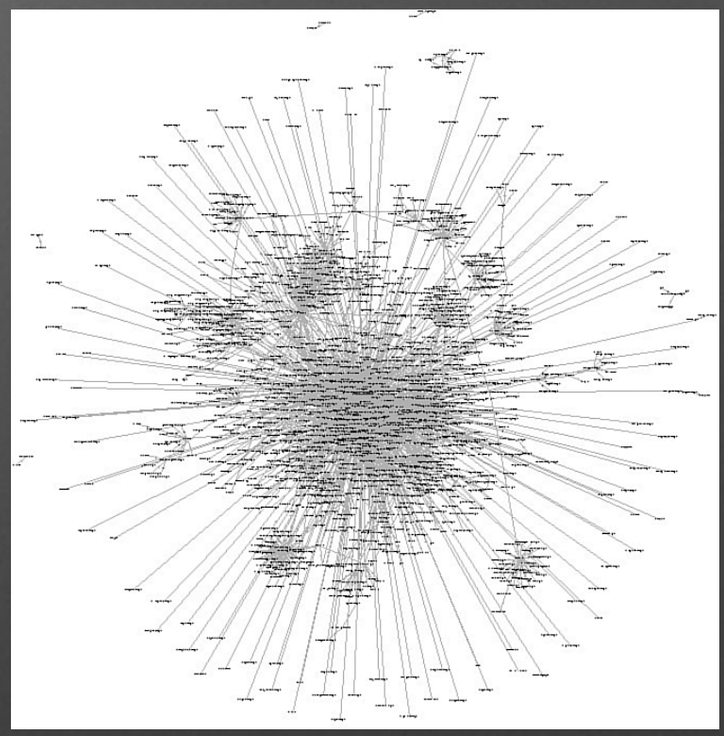
Anthony Winchester
Birmingham-Southern College

Blown to Bits: Chapter 5

http://www.dcbar.org/blog/post.cfm/encryption-for-lawyers-legal-tech

Privacy

1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
*
0 +
#




I-35 N: US-169
Construction 0 mi. away
Length
4.7

Needs for Privacy and Security

- Protection from against external/internal hackers
- Defending against industrial espionage
- Protecting E-commerce assets
- Verifying bank accounts/electronic transfers
- Securing intellectual property
- Preventing issues regarding liability
- Ubiquity of email/networks and privacy
- Cloud-based storage of private information
- Insecure technologies (e.g., wireless)
- Emergence of a paperless society

Question

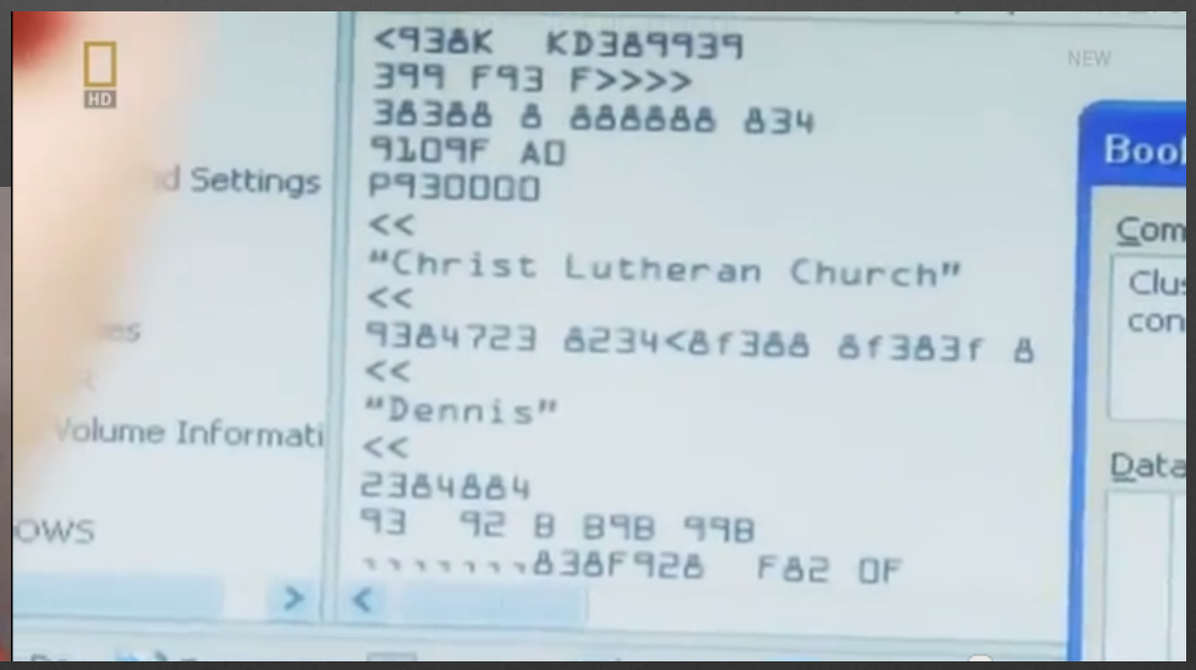
- MIT's Ron Rivest - leading cryptographer
- Should people be able to conduct private conversations, immune from government surveillance, even when that surveillance is fully authorized by a Court order?

Criminals Caught by Bits

Video:

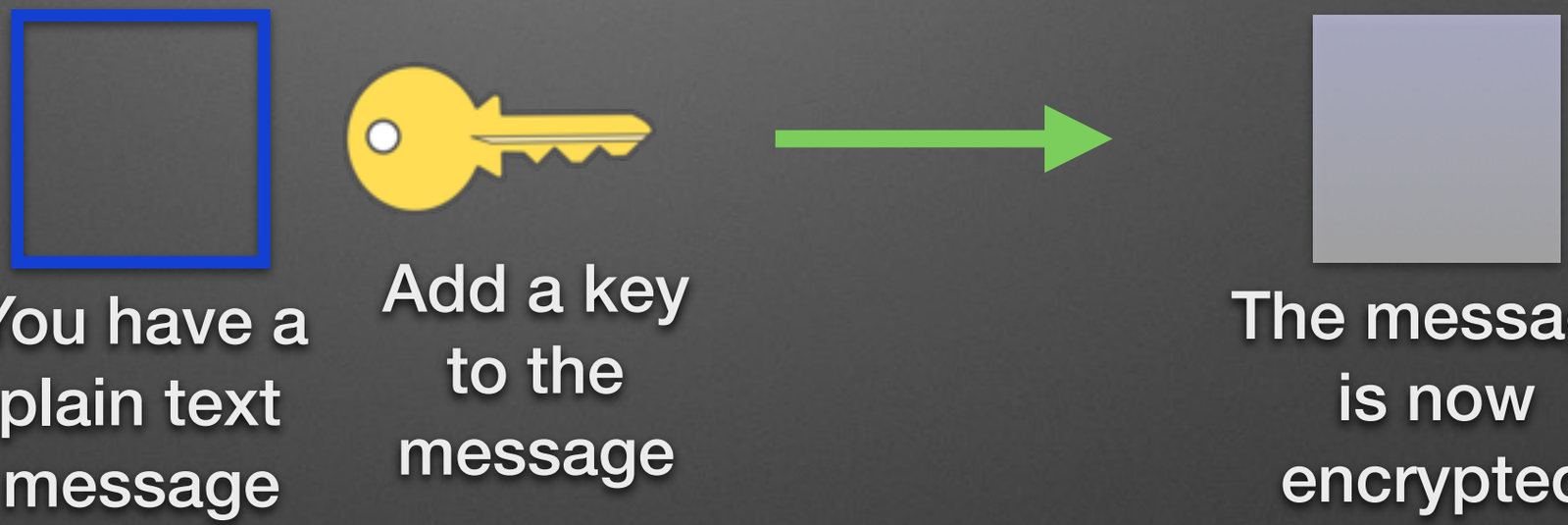
34:40 – 35:10

https://www.youtube.com/watch?v=VPNeIJIPDn0

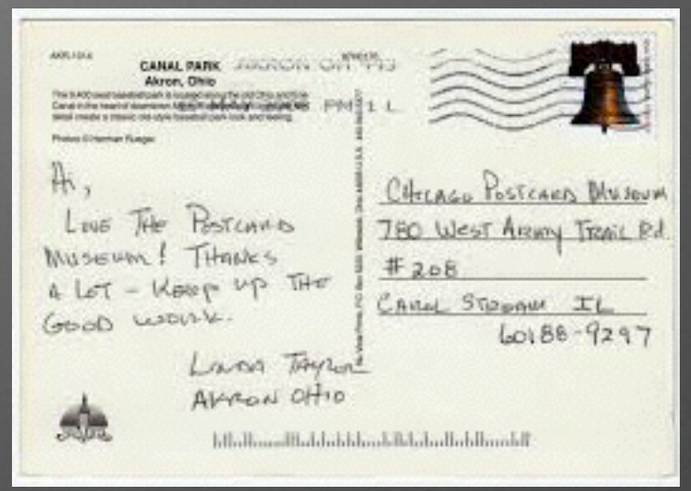


Encryption

- Encryption is the art of encoding messages so they can’t be understood by eavesdroppers

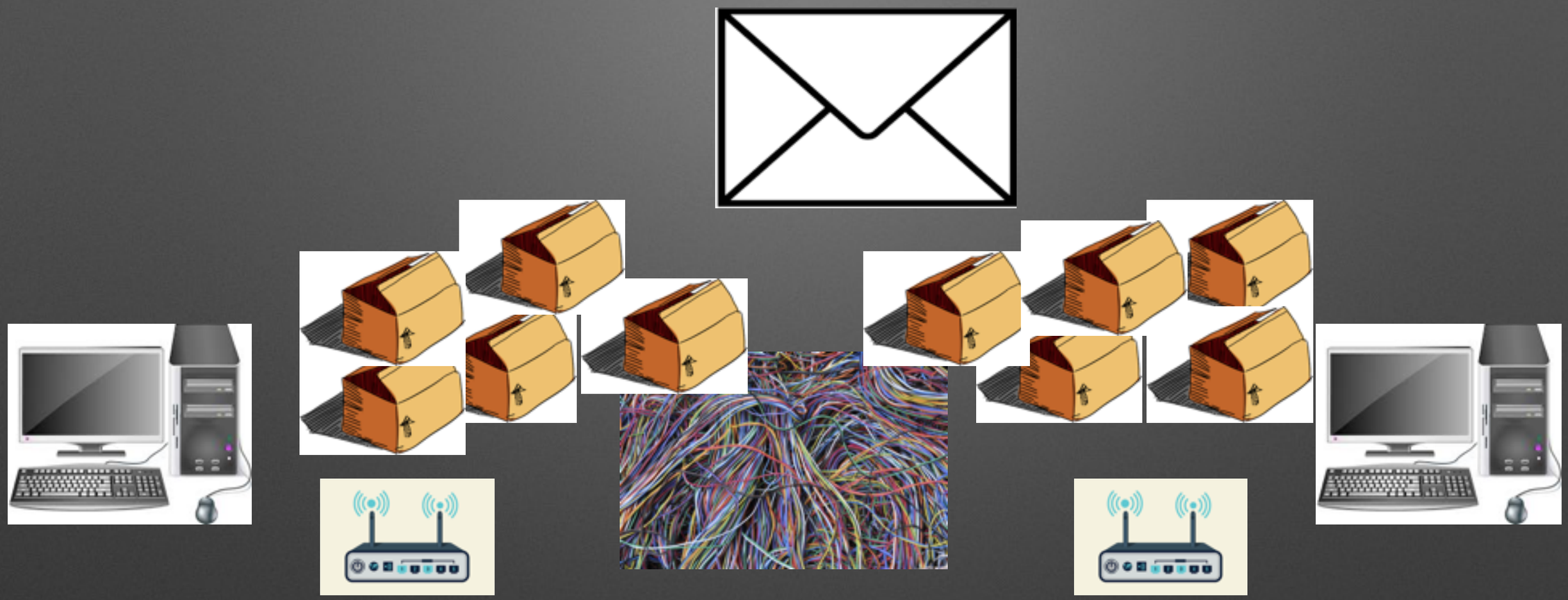


How Data is Transferred



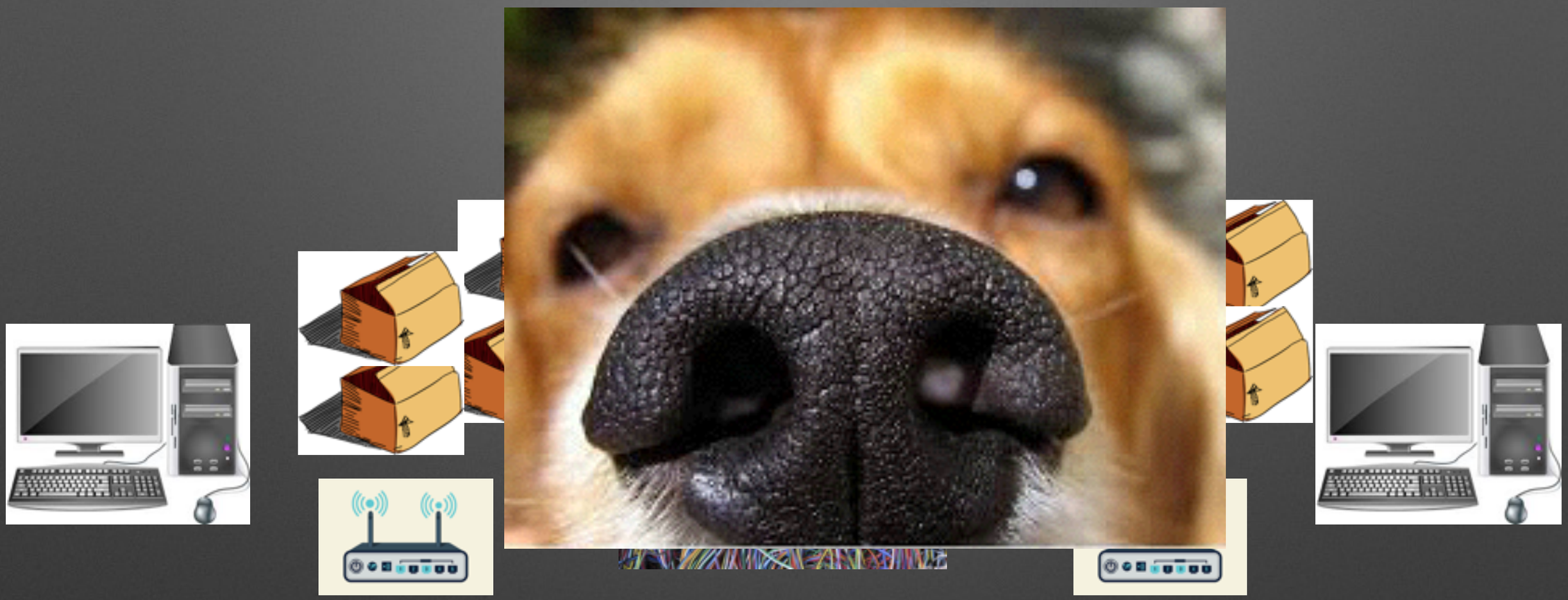
What's the difference between sending a letter in a sealed envelope versus sending a postcard? Anyone who comes across your postcard can read the message (this is sending your mail without encryption). The sealed envelope is similar to encrypting your message, only the recipient can read it.

How Data is Transferred



When you send an email, it goes from your computer through a router, which breaks the email up into different packets (small chunks, which makes it easier to send). Those packets are sent through wires (not all on the same path) that direct the email to it's address (another router). The second router reassembles the packets, and the person on the other end can read the email, which seem secure until…

How Data is Transferred



Someone puts a sniffer on the line. This sniffer is like the credit card reader that malicious individuals put on ATMs and gas pumps. The sniffer actually sniffs out the information being passed along certain routes. If the data is encrypted, the sniffer can't read it.

History

- 50 B.C.Julius Caesar uses cryptographic technique
- 1466 Leon Alberti develops a cipher disk
- 1861 Union forces use a cipher during Civil War
- 1919 Germans develop the Enigma machine for encryption
- 1942 Navajo windtalkers help with secure communication during WWII
- 1948 Claude Shannon develops statistical methods for encryption/decryption
- 1976 IBM develops DES
- 1976 Diffie – Hellman develop public key / private key cryptography
- 1977 Rivest – Shamir – Adleman develop the RSA algorithm for public key / private key

Encryption as a Weapon

- We used to use encryption as a weapon
  - State Department (1990s) demanded encryption researchers were registered as international arms dealers
  - Senator Judd Gregg wanted to create legislation to require encryption to be registered with government agencies holding the keys
- Legislation never went through…all efforts stopped

What Happened?

- Thanks to the explosion of the world wide web, particularly, electronic commerce, encryption became more like an armored car

- Every business and every consumer needed encryption to protect personal information

Encryption Methodologies

- Ciphers - there are many types of ciphers that exist and have been used for hundreds of years usually to protect communications during times of war. The most common type of cipher is a shift cipher or caesar cipher. Check out the Khan Academy tutorial on ciphers vs. codes. I'm only asking you to read the first two sections, but you're welcome to continue.

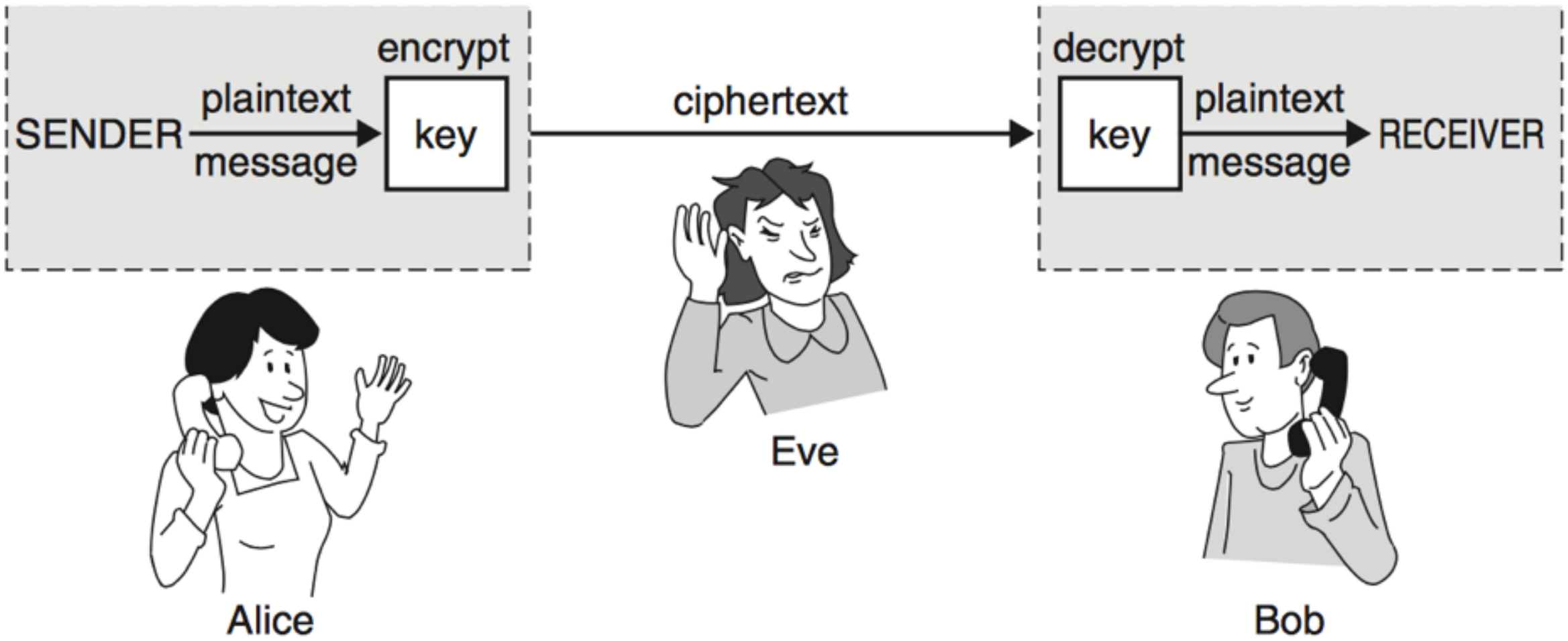
- Khan Academy tutorial on ciphers vs. codes: https://www.khanacademy.org/computing/computer-science/cryptography/ciphers/a/ciphers-vs-codes

- Having read about the shift cipher, can you crack the following?

  - KDSSBDPRQGDB

Encryption Methodologies

- 1976: Public key encryption - still works today, check out the video below explaining the process



https://www.khanacademy.org/computing/computer-science/internet-intro/internet-works-intro/v/the-internet-encryption-and-public-keys

Basic Terminology

- Cryptography deals with creating documents that can be shared secretly over public communication channels
- Cryptographic documents are decrypted with the key associated with encryption, with the knowledge of the encryptor
- The word cryptography comes from the Greek words: Krypto (secret) and graphein (write)
- Cryptanalysis deals with finding the encryption key without the knowledge of the encryptor
- Cryptology deals with cryptography and cryptanalysis
- Cryptosystems are computer systems used to encrypt data for secure transmission and storage

Basic Terminology

- Plaintext is text that is in readable form
- Ciphertext results from plaintext by applying the encryption key
- Notations:
  - M message, C ciphertext, E encryption, D decryption, k key
  - E(M) = C
  - E(M, k) = C
- Fact: D(C) = M, D(C, k) = M
- Thus: D(E(M)) = M

Since we're talking about ciphers and codes, let's talk about Alan Turing for a Who's Who…

Alan Turing

June 1912 - June 1954

- Created the Turing Machine (1936)
  - Universal machine capable of computing anything that is computable
  - Foundation for modern computer
- Studied cryptology at Princeton (PhD)
  - Worked for Government Code and Cypher School, a British code-breaking organization

Alan Turing

June 1912 - June 1954

- Code breaker during part of WWII working on Ultra intelligence
    - He sped up the process of breaking German ciphers by making improvements to the Polish bombe system – an electromechanical device used to help decipher German Enigma encrypted signals
    - His work was so impactful and top secret that two papers were just released from government in 2012
- He then worked for the National Physical Library - London (1940s)
    - His focus was on the Automatic Computing Engine
- He then went to the University of Manchester (1950s)
    - Where he focused on Artificial Intelligence. He developed the Turing Test, which is still thought of as the way to distinguish artificial intelligence – the test is to have a computer and a human answering questions asked by a tester. If the tester can't distinguish the human from the computer, that computer is considered intelligent.

Alan Turing

June 1912 - June 1954

- During his artificial intelligence research, he asked:
  - "I propose to consider the question, 'Can machines think?’"
    - "Are there imaginable digital computers which would do well in the imitation game?” (The imitation game had to do with gender, but it related back to the Turing Test idea – could a computer imitate a human).
- ACM started the Turing Award in 1966 in Turing’s honor
- Check out this site if you’d like to learn more: https://www.biography.com/people/alan-turing-9512017

Cool Application of Cryptography

- Steganography is the method of hiding secret messages in an ordinary document
- Steganography does not use encryption explicitly, but rather through hiding information into an existing document
- Steganography does not generally increase file size for hidden messages
- Example: select the bit patterns in pixel colors to hide the message


THANKFUL

Challenge