Cryptography Part I

Cryptographic Hardware for Embedded Systems
ECE 3170 A

Fall 2024

Assoc. Prof. Vincent John Mooney III

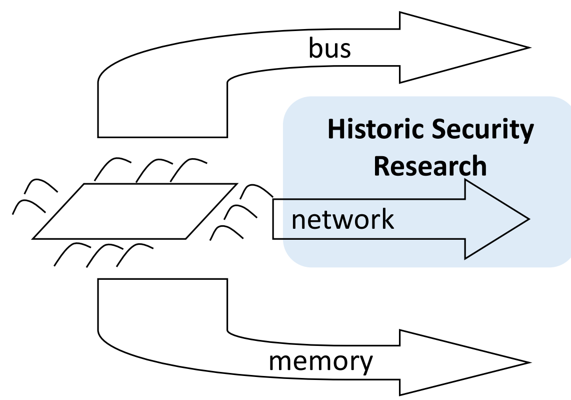
Georgia Institute of Technology

Reading

- Please read chapters 1 and 7 of the course textbook by Schneier

Cryptography

- Cryptography is the science of keeping communication private
  - More formally, cryptography is traditionally defined as secure communication over an insecure channel



Security

- Notice that the definition of cryptography utilizes the definition of security
- A typical dictionary definition of security would say that it is freedom from danger or freedom from fear of being hurt

Secure from What Threat?

- Traditionally, in security research the perceived threats are clearly defined
- The threats of concern form an "attack surface"

Kerckhoffs' Principle

- Auguste Kerckhoffs (1835-1906) was a Professor of Languages who carried out research in linguistics and cryptography
- He was a fan of constructed (i.e., non-societal) languages
- In 1883 he published two articles in which he claimed that it is very important that a cryptographic method still work even if the technique falls into enemy hands
  - The method will rely on a *key* (e.g., a sequence of characters including numbers, etc.) which should not be provided to the enemy
  - The method should be portable, e.g., should not require very large equipment difficult to transport quickly and reliably
  - The method itself should not be required to be a secret: "The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience."

Terminology

- Plaintext or cleartext: the message in a language understood by both the sender (Alpha) and the receiver (Buzz)
- Encryption: the process of disguising a message such that it cannot be recognized by an adversary
- Ciphertext (also cyphertext): the encrypted message
- Decryption: the process of transforming ciphertext back into the original plaintext
- Key: information, usually a number, known to the communicating parties but not to any adversaries – a key is a *secret*

Traditional Cryptanalytic Attacks

1) Ciphertext only attack
   - Cryptanalyst has the ciphertext $\{C_i\}$ of a number of messages
     - $C_1 = E_k(P_1)$, $C_2 = E_k(P_2)$, …
2) Known plaintext attack
   - Cryptanalyst has a number of plaintext, ciphertext pairs
     - $(P_i, C_i) \mid C_i = E_k(P_i)$
   - May also have additional ciphertext without associated plaintext
3) Chosen plaintext attack (CPA)
   - Cryptanalyst can obtain ciphertext for chosen plaintext
   - Given P_i, $C_i = E_k(P_i)$ can be found

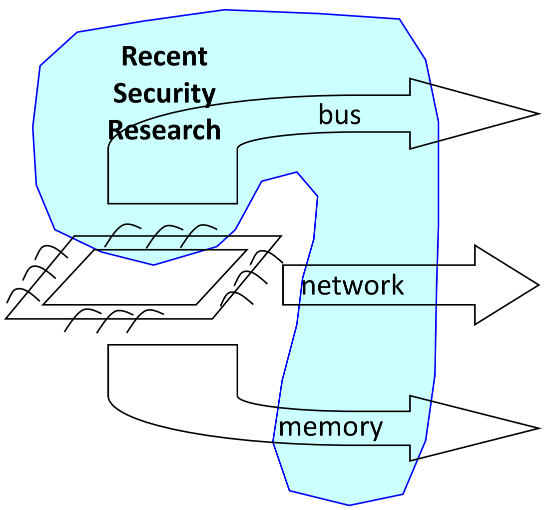
- Goals include decryption of specific messages and deduction of the key

Traditional Cryptanalytic Attacks (continued)

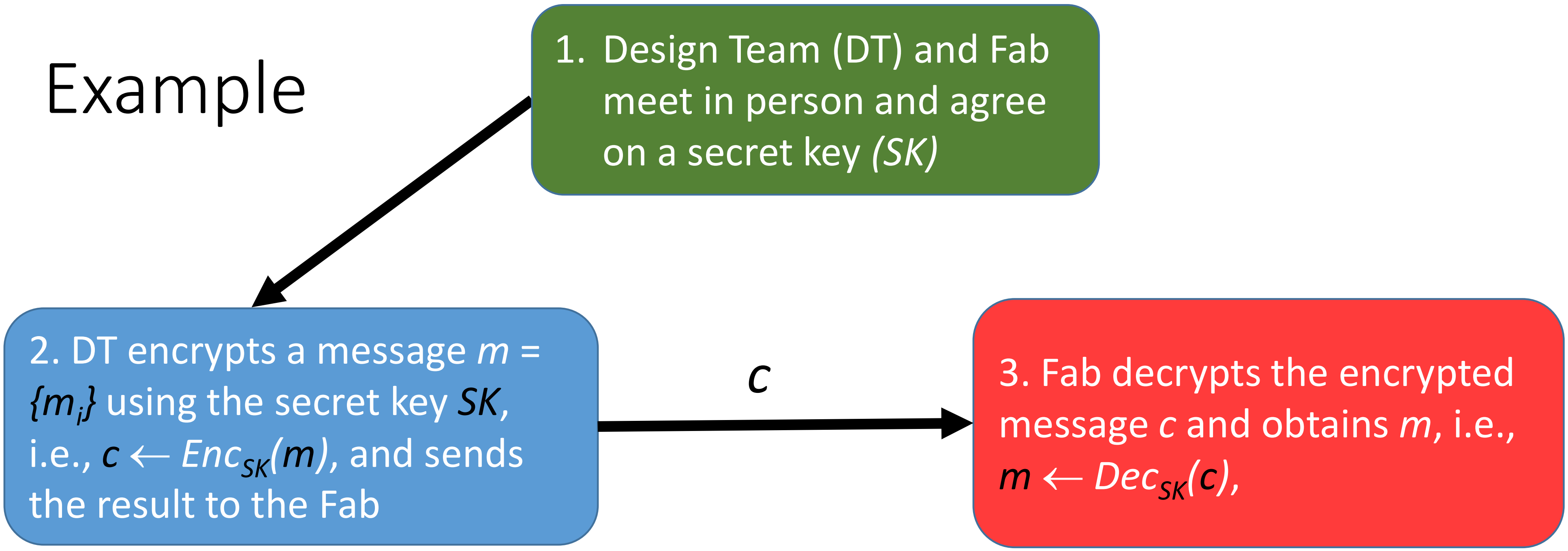
4) Chosen ciphertext attack (CCA)
    - Cryptanalyst can obtain plaintext for (some) chosen ciphertext
    - Given C_i, P_i | $C_i = E_k(P_i)$ can be found for some (or all) cases

- The primary goal is the deduction of the key; in the case that only some plaintext can be decrypted, another goal may be decryption of specific messages not able to be decrypted via chosen ciphertext
- Note that these four traditional attacks are listed by increasing capability of the cryptanalyst, i.e., case (1) is the weakest whereas case (4) is the most capable

Modern Cryptography



Example


1. Design Team (DT) and Fab meet in person and agree on a secret key *(SK)*
2. DT encrypts a message $m = \{m_i\}$ using the secret key SK, i.e., $c \leftarrow Enc_{SK}(m)$, and sends the result to the Fab
c
3. Fab decrypts the encrypted message c and obtains m, i.e., $m \leftarrow Dec_{SK}(c)$,

Data Encryption Standard (DES)

- In 1973, NIST (the National Institute of Standards and Technology – technically, however, in 1973 NIST was named the National Bureau of Standards) issued a public request for a standard cryptographic algorithm
  - High level of security dependent only on the key
  - Completely specified and easy to understand
  - Publically available
  - Usable in diverse application scenarios
  - Efficient & economical to implement in hardware
  - Validated & tested

Some Interesting Historical Facts

- The capture of a version of the Enigma machine helped crack the German cryptographic codes in WWII

Some Large Numbers

- Odds of being killed by lightning (per day): 1 in 9 billion (2^{33})
- Odds of being killed in a car accident
  - In a particular year (e.g., in the U.S. in 1993): 1 in 6100 (2^{12})
  - In an entire lifetime: 1 in 88 (2^{7})
- Time until the sun goes nova: 10^{9} (2^{30}) years
- Age of the universe: 10^{10} (2^{34}) years
- Number of atoms in the sun: 10^{57} (2^{190})
- Number of atoms in the universe (excl. dark matter): 10^{77} (2^{265})
- Volume of the universe: 10^{84} (2^{280}) cm^3
- NOTE: the above numbers are “ballpark,” e.g., $2^{12} = 4096$ (not 6100)