L8: Cipher Techniques: Problems

Hui Chen, Ph.D.

Dept. of Engineering & Computer Science

Virginia State University

Petersburg, VA 23806

Acknowledgement

☐ Many slides are from or are revised from the slides of the author of the textbook

- Matt Bishop, Introduction to Computer Security, Addison-Wesley Professional, October, 2004, ISBN-13: 978-0-321-24774-5. [Introduction to Computer Security @ VSU's Safari Book Online subscription](#)

- http://nob.cs.ucdavis.edu/book/book-intro/slides/

Outline

- ☐ Precomputing possible messages
- ☐ Misordered blocks
- ☐ Statistical regularities

Use Ciphers: A Challenge

- Cryptographic systems are sensitive to the environment they are being used

- Using cryptographic systems over a network introduces problems

- Using a good cipher is not enough, how to use the cipher matters greatly

- What can go wrong if we naively use ciphers?

Threats in Network Environment

- ◻ Knowledge of the environment and threats in the environment
  - ◼ Is the set of possible messages small?
  - ◼ Do the messages exhibit regularizes that remain after encipherment
  - ◼ Can an active wiretapper rearrange or change parts of the message?
- ◻ Three common problems
  - ◼ Precomputation, misordered blocks, and statistical regularities

Attack 1. Precomputation

❑ Precomputing possible messages or *forward searches*

❑ Set of possible messages *M* small

❑ Public key cipher *f* used

❑ Idea: precompute set of possible ciphertexts *f(M)* and build table *(m, f(m))* where $m \in M$

❑ When ciphertext *f(m)* appears, use table to find *m*

Forward Search Attack: Example

- Cathy knows Alice will send Bob one of two messages using a Public Key Cryptosystem
  - Enciphered BUY or enciphered SELL
- Using public key e_{Bob}, Cathy precomputes a table
  - $c_1 = f(m_1) = \{BUY\}_{e_{Bob}}$
  - $c_2 = f(m_2) = \{SELL\}_{e_{Bob}}$
- Looking up intercepted enciphered message, Cathy sees Alice send Bob m_2.
- Cathy knows Alice send SELL

Obscure Threats

- Example: digitized sound (Simmons, 1982)
  - Initial calculations suggest 2^{32} such plaintexts
  - Seems like far too many possible plaintexts
  - Analysis of redundancy in human speech reduced this to about 100,000 ($\approx 2^{17}$)
  - This is small enough to worry about precomputation attacks

Notes on Precomputation

- **Chosen plaintext attack against symmetric crytosystems**
  - Derive key
  - e.g., Hellman, 1980
- **Precomputation attack against public key crytosystems**
  - Drive plaintext messages
  - Does not reveal private key

Misordered Blocks

❑ Parts of a ciphertext message can be deleted, replayed or reordered (Denning, 1982)

Misordered Blocks: Example

- Alice sends Bob message
  - n_{Bob} = 77, e_{Bob} = 17, d_{Bob} = 53
  - Message is LIVE (11 08 21 04)
  - Enciphered message is 44 57 21 16
- Eve intercepts it, rearranges blocks
  - Now enciphered message is 16 21 57 44
- Bob gets enciphered message, deciphers it
  - He sees EVIL

Notes on Misordered Blocks

□ **Digitally signing each block will not stop this attack**

  ■ The parts are not bound to one another

□ **Two approaches to counter the attack**

  1. Generate a cryptographic checksum of the *entire* message and sign it

  2. Place sequence numbers in each block of message, so recipient can tell intended order. Then you sign each block

Statistical Regularities

❑ If plaintext repeats, ciphertext may too

Statistical Regularities: Example

◻ Example using DES:

- input (in hex):

  3231 3433 3635 3837 3231 3433 3635 3837

- corresponding output (in hex):

  ef7c 4bb2 b4ce 6f3b ef7c 4bb2 b4ce 6f3b

Notes on Statistical Regularities

☐ Code book mode (CBM)

- Each part is enciphered separately, so the same plaintext always produces the same ciphertext
- Each part is effectively looked up in a list of plaintext-ciphertext pairs
- It is the cause of the statistical regularity

☐ Approach to counter the attack

- Cascade blocks together (chaining, more details later)

What These Mean

- Use of *strong* cryptosystems, *well-chosen* (or random) keys *not enough* to be secure
- Other factors:
  - Protocols directing use of cryptosystems
  - Ancillary information added by protocols
  - Implementation (not discussed here)
  - Maintenance and operation (not discussed here)

Summary

❑ Discussed three attacks

- Precomputation (forward search)
- Misordered blocks
- Statistical regularities

❑ Strong cryptosystems and random keys not enough

❑ Careful engineering matters