Crypto IX: Key Length

Cryptographic Hardware for Embedded Systems

ECE 3170

Fall 2025

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Reading Assignment

- Please read Chapter 7 of the course textbook by Schneier

Notation from Katz and Lindell

- $\{X\}$ is a set of elements of type X
- m is a message in plaintext
  - m is composed of smaller blocks m_i suitable for individual encryption steps
  - $m = \{m_i\}$
- c_i is ciphertext corresponding to message block m_i
- c is ciphertext corresponding to message m
- Enc_k is encryption with key k
  - $c \leftarrow Enc_k(m)$
- Dec_k is decryption with key k
  - $m \leftarrow Dec_k(c)$
- MAC_k is generation of a message authentication code t with key k
  - $t \leftarrow Mac_k(m)$ or, alternatively, $t \leftarrow Mac_k(c)$
- $<a,b>$ is a concatenation of a followed by b

Notation from Schneier

- C_i is ciphertext message i
- P_i is plaintext message i
- E_k is encryption with key k
  - Note that E could be symmetric or asymmetric
  - $E_k(P_i) = C_i$
- D_k is decryption with key k
  - Note that D could be symmetric or asymmetric
  - However, for asymmetric cryptographic, need distinct keys
    - E_{k1} and D_{k2} where *k1* is the public "key" and *k2* is the private "key"
    - $E_{k1}(P_i) = C_i$
    - $D_{k2}(C_i) = P_i$
- $\{X\}$ is a set of elements of type X
- | is "such that"; e.g., integer i | $3 < i < 5$ implies that $i = 4$

Key Length

- Security depends on the *inability* of the adversary to decrypt without the secret
- The *secret* is the key
- The inability of the adversary to decrypt is based to a large extent on the *length* of the key

Cryptanalysis

- Traditionally, the adversary is assumed to have complete access to communications
  - Cryptographic algorithm is known
  - Key is not known
- Non-academic approaches may also relay on not revealing the cryptographic algorithm, i.e., secrecy of the algorithm as well as the key
  - So-called “security by obscurity”
  - However, there are strong arguments against this
    - Auguste Kerckhoffs, born in the Netherlands, argued in the late 19th Century, “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.”

Recall from Cryptography Part I Lecture

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

Cryptanalysis (continued)

- Known plaintext attack capability more common than you might think
- May obtain plaintext by some other means and then intercept the ciphertext
  - A document file may have a standard header
  - A database may have a standard record format or directory beginning
  - Email messages may begin in a standard way
  - And many more…

Cryptanalysis (continued some more!)

- Consider a symmetric encryption scheme and the known plaintext attack
  - If the "strength" of the cryptographic algorithm is "perfect," then knowledge of the algorithm reveals nothing advantageous to the cryptanalyst
  - Therefore, since the key is not known, the only approach left open to the cryptanalyst is "brute force"
  - For a key of *n* bits, a brute force attack simply tries out each key one by one
    - After 2^{n-1} tries, there is approximately a $\frac{2^{n-1}}{2^n}$ = 50% chance of discovering the key
- Consider a 56-bit key
  - Further consider a GHz machine able to make 10^9 comparisons per second
  - 2^{55} = 36,028,797,018,963,968 comparisons $\cong$ 36,028,797 seconds $\cong$ 1.15 years
    - $\Rightarrow$ 50% chance of discovering the key in 1.15 years
    - (if only 10^6 comparisons per second, e.g., as in 1995, then require 1150 years for a 50% chance)
  - However, 64 bits requires 589 years, and 128 bits requires 10^{22} years
    - The universe is only 10^{10} years old!

How “Strong” is a Cryptographic Algorithm?

- Typically assume a known plaintext attack
  - Ability to withstand a chosen plaintext attack (CPA) is better
- DES and AES are considered to be strong against known attacks
  - However, due to its 56-bit key, DES is no longer considered to be safe against a cryptanalyst with sufficient compute power to carry out enough (2^{56}) brute-force comparisons
  - AES has three key size options: 128 bits, 192 bits and 256 bits
  - Triple DES (3DES) uses three 56-bit keys *k1*, *k2* and *k3*
    - $C_i = E_{k3}(D_{k2}(E_{k1}(P_i)))$
    - $P_i = D_{k1}(E_{k2}(D_{k3}(C_i)))$
    - Due to some known ways to optimize the key search under the known plaintext attack, the number of comparisons required is not $(2^{56})(2^{56})(2^{56})$ but rather is $2^{2*56} = 2^{112}$

Symmetric versus Asymmetric Key Length

- Asymmetric cryptography using the RSA algorithm does not involve using all possible key bitstrings
  - Instead, RSA relies on the difficulty of trying to factor a very large number
- Can estimate that a 128-bit AES key has equivalent security (i.e., difficulty of discovering the key under a known plaintext attack) of a 2048-bit RSA private key