Justin Ciocoi

Oct. 12, 2023

CSCI 360 Textbook Notes

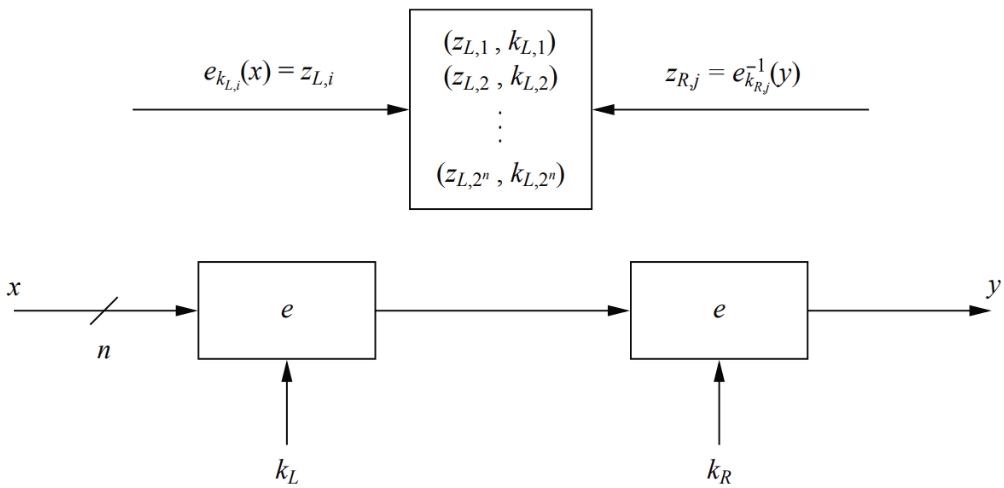
Cryptography and Cryptanalysis

Increasing the Security of Block Ciphers

- Generally speaking, there are two broad methods by which a block cipher which may not be considered secure can be strengthened to conform to modern cryptographic standards
    - *Multiple Encryption*, where encryption is conducted multiple times consecutively
    - *Key Whitening*

5.3.1: Double Encryption and Meet-in-the-Middle Attack

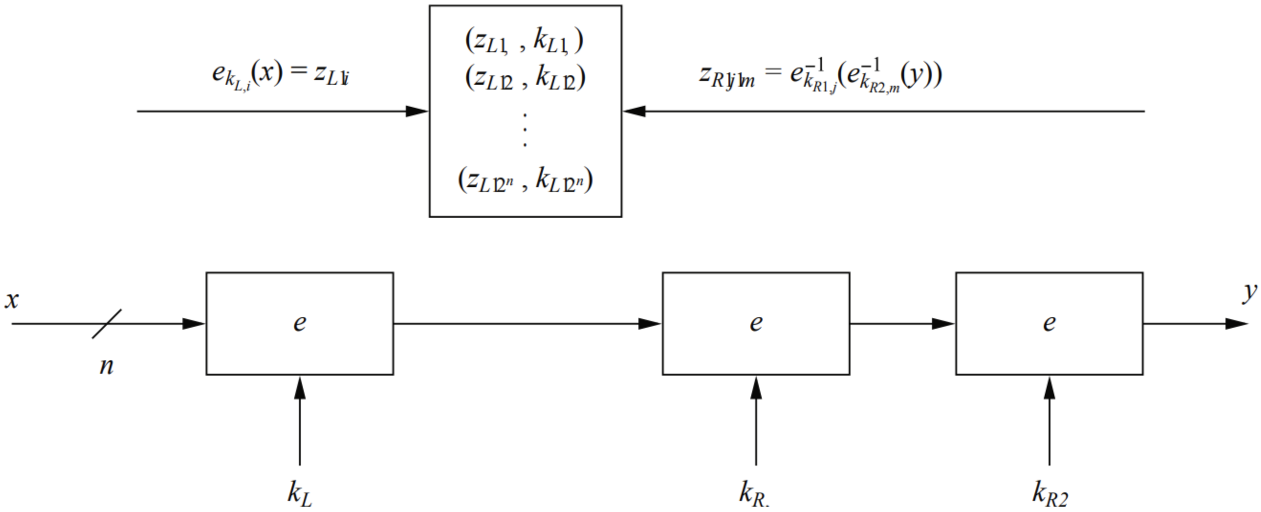
- Let us assume we have a block cipher of key length κ bits
- In *double encryption*, plain-text, x, is encrypted using key k_L, and the resulting cipher-text is encrypted again using a second key k_R



- In order to brute force a double encryption, the effective key length would be 2κ and an exhaustive key search would require $2^{\kappa} \cdot 2^{\kappa} = 2^{2\kappa}$
- In a *meet-in-the-middle attack*, the attacker can first crack the left hand side, and then the right hand side
  - The total complexity here is $2^{\kappa} + 2^{\kappa} = 2 \cdot 2^{\kappa} = 2^{\kappa+1}$
  - This is barely more complex than breaking the single encryption
  - **Attack Phase 1 Table Computation:** For plaintext, x_1, compute a lookup table for all pairs $(k_{L,i}, z_{L,i})$, where $e_{k_{L,i}}(x_1) = z_{L,i}$, and $i = 1, 2, \cdots, 2^{\kappa}$
    - The $z_{L,i}$ are the intermediate values that occur between the two encryptions
  - **Attack Phase 2 Key Matching:** Now, we check all possible keys starting with the all 0 key until we see a collision of two values, i.e. $z_{L,i} = z_{R,j}$
    - This means there exists a key pair $(k_{L,i}, k_{R,j})$
    - A second plain-text cipher-text pair must be checked since there are multiple possible keys that could do the correct encryption for a single pair
- ***Theorem 5.3.1:*** Given l subsequent encryptions of a block cipher with key length κ bits and block size of n bits, as well as t cipher-text, plain-text pairs, $(x_1, y_1), \cdots, (x_t, y_t)$
  - The expected number of false keys which encrypt all plain-texts to the corresponding cipher-texts is $2^{l\kappa - tn}$

5.3.2: Triple Encryption

- Compared to double encryption, *triple encryption* is *far more secure*
- For compatibility in use with certain legacy systems, triple encryption is sometimes done in the form $y = e_{k1}(e_{k2}^{-1}(e_{k3}(x)))$
  - If $k_1 = k_2$, then the operation is essentially the same as single encryption in the form $y = e_{k3}(x)$
- A meet-in-the-middle attack can still occur, as shown below



- The strength of triple encryption can be seen that regardless of which intermediate cipher-text an attacker chooses to compute a lookup table for, the attacker will have to crack a key of double length for one of the sides

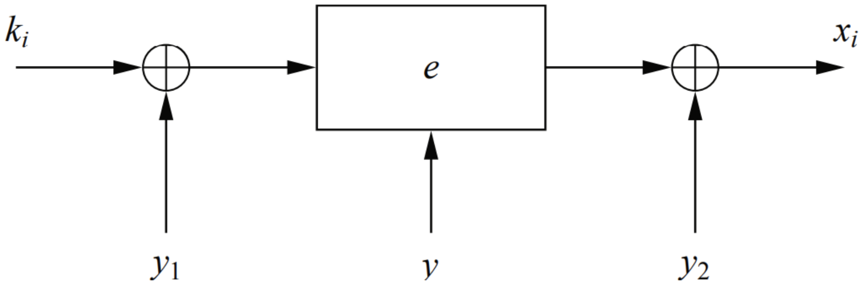
- The meet in the middle attack makes triple encryption as secure as an un-attacked double encryption

---

5.3.3: Key Whitening

- A simple technique known as *key whitening* makes it possible to make block ciphers such as DES far more resistant to brute-force attacks

- In addition to the standard cipher key, k, two *whitening keys*, k_1 and k_2 are used to $\oplus$-mask the plain-text and cipher-text



- **Formal Definition of Key Whitening for Block Ciphers:**
  - *Encryption:* $y = e_{k,k_1,k_2}(x) = e_k(x \oplus k_1) \oplus k_2$
  - *Decryption:* $x = e^{-1}_{k,k_1,k_2}(x) = e^{-1}_k(y \oplus k_2) \oplus k_1$

- Key whitening does not prevent against analytical attacks, but rather works to strengthen ciphers whose key space is too small
    - An example of this is DESX