CS2107 Tutorial 2 (Encryption: One-Time Pad & Block Ciphers)

School of Computing, NUS

30 August – 3 September 2021

1. *Attackable OTP? (Mid-Term Quiz S1 AY2019/20):*
   Bob really likes the One-Time Pad (OTP), an encryption scheme that does achieve perfect security. Bob thinks that he should be able to use the OTP by itself for a *secure message communication*, and not just for preserving confidentiality.

   Suppose Bob's OTP keys are random and always fresh as required. His plaintexts, however, always start with "`From: Bob`" string, and this is known by Mallory. Mallory is a man-in-the-middle, who can intercept Bob's ciphertexts, modify them, and then relay the modified ciphertexts to the respective receivers.

   Suppose now Mallory wants to modify all Bob's OTP ciphertexts so that, when decrypted by their respective receivers using correct keys, the recovered plaintexts start with "`From: Bot`" instead. What should Mallory *turn each OTP ciphertext from Bob into*? Explain briefly why your attack works.

   (Note: Suppose the two relevant characters are encoded using their following ASCII-based binary strings: '`b`' $\rightarrow$ 0110 0010, '`t`' $\rightarrow$ 0111 0100.)

2. *Block Cipher with a Small Block Size:*
   Bob is designing a block cipher that performs complex operations similar to those in AES. He believes that he can combine the strengths of both block cipher (e.g. high confusion and diffusion) with that of stream cipher (e.g. lower latency) if he makes the block size rather small. Hence, he sets the size of the input and output blocks of his cipher to **16 bits** only. Alice, however, warns Bob that his block cipher can be attacked due to its small block size.

   (a) Consider a *known-plaintext attack* scenario, where an attacker can learn a number of plaintext and ciphertext pairs encrypted using the same key. Suppose the attacker wants to implement a *codebook attack* on Bob's Cipher, which is a block cipher with a small block size, by compiling a lookup table of all plaintext-ciphertext pairs observed under the same key. How much storage will the attacker need to comprehensively store *all the input and output blocks* in his table? Express your answer in MB (megabyte) or GB (gigabyte).
   Note: 1MB = 2^{20}, 1GB = 2^{30}.

   (b) Given Alice's warning and posssible codebook attack, Bob agrees to increase the size of the input and output blocks of his cipher to **48 bits**. Using the same codebook attack, how much storage will the attacker now need to store *all the input and output blocks* in his lookup table? Express your answer in MB (megabyte), GB (gigabyte), TB (terabyte), or PB (petabyte).
   Note: 1T = 2^{40}, 1P = 2^{50}.

3. *Mode-of-Operation (Mid-Term Quiz S1 AY2018/19):*
Cipher Block Chaining (CBC) mode-of-operation is commonly used to encrypt a plaintext longer than a ciphers block. In CBC, each plaintext block is XOR-ed with the previous ciphertext block before being encrypted. An IV is used in encrypting the first plaintext block.

   Mathematically, the encryption can thus be expressed as follows:
   Given a n-block plaintext message x_1, x_2, x_3, ..., x_n, a secret key K, and an initial value IV, CBC outputs $(n+1)$-block ciphertext message y_0, y_1, y_2, ..., y_n, where:

   - $y_0 = IV$;
   - $y_k = Enc_K(x_k \oplus y_{k-1})$, for $k = 1, 2, 3, \ldots, n$.

   Given the definition above, answer the following questions:

   - Your lecture notes show a diagram depicting how a CBC-based encryption is done. Draw a diagram of the corresponding CBC-based *decryption*.
   - How is decryption affected if the first ciphertext block y_0 is *removed* from the ciphertext?
   - Can the encryption processes of different blocks belonging to a plaintext run *in parallel*? How about the decryption of a ciphertext's different blocks?

4. *Insecure Use of DES (Mid-Term Quiz S1 AY2018/19):*

   (a) Bob knows that DES has a rather short key size/length of 56 bits. He, however, still wants to employ DES due to its widespread availability. Bob thinks that he has found a good way of addressing the limited key length of DES by randomly selecting three different keys K_1, K_2 and K_3. Bob then performs his DES encryption as follows:

   $$C = E_{K_1 \oplus K_2 \oplus K_3}(P).$$

   Decryption process is then performed using $K_1 \oplus K_2 \oplus K_3$ as its key. Bob argues that his method significantly increases the key space size. Is Bob's argument correct? Argue concisely by comparing the key space size of using one and three keys above.

   (b) Bob now uses only two secret keys K_1 and K_2. However, he modifies his encryption to implement 2DES as follows:

   $$C = E_{K_2}(E_{K_1}(P)).$$

   Bob now believes that his double-encryption method indeed *doubles* the key space size to $2^{2.56} = 2^{112}$, and brute-forcing correspondingly requires 2^{112} cryptographic operations. How can you tell Bob that, under the **known-plaintext attack**, there is a way to find his two keys by performing $2.2^{56} = 2^{56+1} = 2^{57}$ cryptographic operations only?

5. *3DES Encryption Options:*
   Your lecture notes have mentioned two 3DES encryption options, namely:

   - $E_{k_1}(E_{k_2}(E_{k_1}(x)))$; and
   - $E_{k_1}(D_{k_2}(E_{k_1}(x)))$.

The latter is quite popular due to its extra benefit. It can provide a backward compatibility with the (single) DES. Explain succinctly how one can use 3DES to be compatible with, or simulate, DES.

— End of Tutorial —