Introduction to Cryptography

TEK 4500 (Fall 2020)

Problem Set 3

Problem 1.

Read Chapter 5 in [BR] (Sections 5.6 and 5.8 can be skipped. The proofs in Section 5.7 can be skipped on first reading, but it is recommended to have a look at it).

Problem 2.

An encryption scheme secure according to the IND-CPA definition is not required to hide the length of the plaintext. This is captured in the formal IND-CPA security experiment (see Fig. 1) by checking that the adversary does not submit unequal length messages M_0, M_1 to be challenged on (see Lines 4+5 in Fig. 1). Suppose Lines 4+5 were *not* included in $\mathbf{Exp}^{\mathsf{ind\text{-}cpa}}_{\Sigma}(\mathcal{A})$. Show how you can break *any* encryption scheme $\Sigma = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ that doesn't hide the plaintext length in this variant of IND-CPA.

Problem 3. [Problem 7.2 in [Ros]]

Let $\Sigma = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme having IND$-CPA security (recall that in the IND$-CPA notion ciphertexts are required to be indistinguishable from random strings (see the right-hand experiment in Fig. 2). From Σ define a *new* encryption scheme $\Sigma' = (\mathsf{KeyGen}, \mathsf{Enc}', \mathsf{Dec}')$, where the key generation algorithm is the same, but where the encryption algorithm is defined as

$$\mathsf{Enc}'_K(M) = 00 \| \mathsf{Enc}_K(M),$$

and where Dec' simply throws away the first two bits of the ciphertext and then calls Dec.

a) Does Σ' have IND$-CPA security (according to Fig. 2)? If yes, give a justification; if no, describe an adversary and calculate its IND$-CPA advantage.

b) Does Σ' have IND-CPA security (according to Fig. 1)? If yes, give a justification; if no, describe an adversary and calculate its IND-CPA advantage.

Problem 4.

Show that the CBC and CTR modes-of-operation are *not* IND-CCA secure (see definition in Fig. 3) by describing concrete attacks and calculating their IND-CCA advantages.

$\underline{\mathbf{Exp}^{\mathsf{ind\text{-}cpa}}_{\Sigma}(\mathcal{A})}$

1: $b \leftarrow \{0,1\}$
2: $K \xleftarrow{\$} \Sigma.\mathsf{KeyGen}$
3: $(M_0, M_1) \leftarrow \mathcal{A}^{\mathcal{E}_K(\cdot)}$ ▷ Find stage
4: **if** $|M_0| \neq |M_1|$ **then**
5: **return** $\perp$
6: $C^* \leftarrow \Sigma.\mathsf{Enc}(K, M_b)$
7: $b' \leftarrow \mathcal{A}^{\mathcal{E}_K(\cdot)}(C^*)$ ▷ Guess stage
8: **return** $b' \stackrel{?}{=} b$

$\underline{\mathcal{E}_K(M)}$:

1: **return** $\Sigma.\mathsf{Enc}(K, M)$

$$\mathbf{Adv}^{\mathsf{ind\text{-}cpa}}_{\Sigma}(\mathcal{A}) = \left|2 \cdot \Pr[\mathbf{Exp}^{\mathsf{ind\text{-}cpa}}_{\Sigma}(\mathcal{A}) \Rightarrow \mathsf{true}] - 1\right|$$

Figure 1: IND-CPA security experiment.

$\underline{\mathbf{Exp}^{\mathsf{ind\$\text{-}cpa}}_{\Sigma}(\mathcal{A})}$

1: $b \leftarrow \{0,1\}$
2: $K \xleftarrow{\$} \Sigma.\mathsf{KeyGen}$
3: $b' \leftarrow \mathcal{A}^{\$_b(\cdot)}$
4: **return** $b' \stackrel{?}{=} b$

$\underline{\$_b(M)}$:

1: $C_1 \leftarrow \Sigma.\mathsf{Enc}(K, M)$
2: $C_0 \xleftarrow{\$} \{0,1\}^{|C_1|}$
3: **return** C_b

$$\mathbf{Adv}^{\mathsf{ind\$\text{-}cpa}}_{\Sigma}(\mathcal{A}) = \left|2 \cdot \Pr[\mathbf{Exp}^{\mathsf{ind\$\text{-}cpa}}_{\Sigma}(\mathcal{A}) \Rightarrow \mathsf{true}] - 1\right|$$

Figure 2: IND$-CPA security experiment.

$\underline{\mathbf{Exp}^{\mathsf{ind\text{-}cca}}_{\Sigma}(\mathcal{A})}$

$b \leftarrow \{0,1\}$
$K \xleftarrow{\$} \Sigma.\mathsf{KeyGen}$
$(M_0, M_1) \leftarrow \mathcal{A}^{\mathcal{E}_K(\cdot),\mathcal{D}_K(\cdot)}$
if $|M_0| \neq |M_1|$ **then**
    return $\perp$
$C^* \leftarrow \Sigma.\mathsf{Enc}(K, M_b)$
$b' \leftarrow \mathcal{A}^{\mathcal{E}_K(\cdot),\mathcal{D}_K(\cdot)}(C^*)$
return $b' \stackrel{?}{=} b$

$\underline{\mathcal{E}_K(M)}$:

return $\Sigma.\mathsf{Enc}(K, M)$

$\underline{\mathcal{D}_K(C)}$:

if $C = C^*$ **then**
    return $\perp$
return $\Sigma.\mathsf{Dec}(K, D)$

$$\mathbf{Adv}^{\mathsf{ind\text{-}cca}}_{\Sigma}(\mathcal{A})) = \left|2 \cdot \Pr[\mathbf{Exp}^{\mathsf{ind\text{-}cca}}_{\Sigma}(\mathcal{A}) \Rightarrow \mathsf{true}] - 1\right|$$

Figure 3: IND-CCA security experiment.

Problem 5. [Problem 3.21 in [KL07]]
Let $\Sigma_1 = (\mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\Sigma_2 = (\mathsf{Enc}_2, \mathsf{Dec}_2)$ be two encryption schemes for which it is known that at least one is IND-CPA-secure. The problem is that you don't know which one is IND-CPA-secure and which one may not be. Show how to construct an encryption scheme Σ that is *guaranteed* to be IND-CPA-secure as long as at least one of Σ_1 or Σ_2 is IND-CPA-secure. Give a high-level justification for why your scheme is secure.

Hint 1: Split your original plaintext into two plaintexts so that knowledge about only one reveals *no* information about the original plaintext, but knowledge of both allows you to recover the original plaintext.

Hint 2: Look up secret sharing; in particular, look at Section 3.2 in [Ros].

Problem 6.
The defining equations for CBC encryption are

$$C_0 \xleftarrow{\$} \{0,1\}^n \tag{1}$$
$$C_i \leftarrow \mathcal{E}_K(M_i \oplus C_{i-1}) \qquad i = 1, \ldots, \ell \tag{2}$$

where $\mathcal{E}$ is a block cipher with n-bit blocks. Write the corresponding equations for CBC decryption.

Problem 7. [Problem 5.5 in [BR]]
The CBC-Implicit mode of operation is a CBC variant in which the IV that is used for the very first message to be encrypted is random, while the IV used for each subsequent encrypted message is the last block of ciphertext that was generated (see Fig. 4). The scheme is probabilistic and stateful. Show that CBC-Implicit is insecure by giving a simple and efficient adversary that breaks it in the IND-CPA sense.

Note: Curiously, CBC-Implicit was how CBC was implemented in TLS 1.0. This was patched in TLS 1.1 and higher.

References

[BR] Mihir Bellare and Phillip Rogaway. *Introduction to Modern Cryptography*. https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

[KL07] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC Press, 2007.

[Ros] Mike Rosulek. *The Joy of Cryptography*, (draft Feb 6, 2020). https://web.engr.oregonstate.edu/~rosulekm/crypto/crypto.pdf.

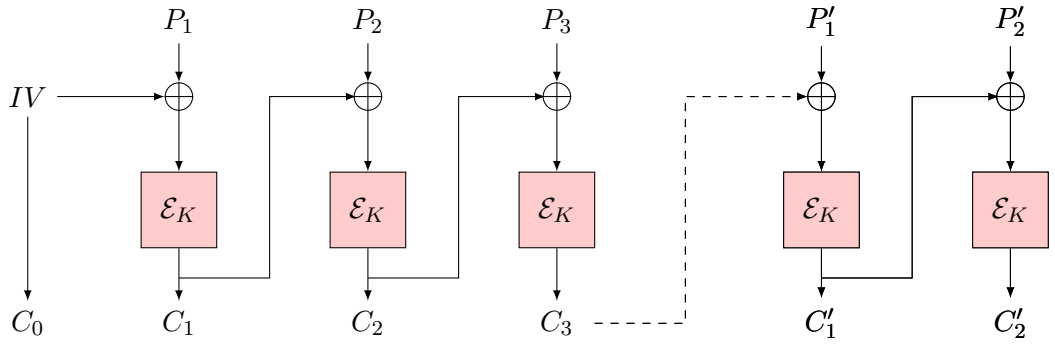

Figure 4: CBC-Implicit mode-of-operation illustrated for two messages $M_1 = P_1 \| P_2 \| P_3$ and $M_2 = P'_1 \| P'_2$. The IV used for the second message is the last ciphertext block of the previous ciphertext, i.e., C_3.