Institute of Computer Science, University of Bern
Cryptography, HS 2019

Prof. Christian Cachin
Luca Zanolini

Exercise 8

8.1 CPA-secure encryption? (3 pts)

Let Σ be an encryption scheme with CPA$ security and derive an encryption scheme Σ' from it, whose encryption algorithm is

$$\Sigma'.\mathsf{Enc}(k, m) = 00||\Sigma.\mathsf{Enc}(k, m).$$

The decryption algorithm of Σ' simply throws away the first two bits of the ciphertext and then calls $\Sigma.\mathsf{Dec}$.

a) Does Σ' have CPA$ security? Prove or disprove (if disproving, show a distinguisher and calculate its advantage).

b) Does Σ' have CPA security? Prove or disprove (if disproving, show a distinguisher and calculate its advantage).

8.2 From a PRP to CPA-secure encryption (4 pts)

Let F be a secure PRP with blocklength λ. Below are several encryption schemes, each with $K = M = \{0,1\}^\lambda$ and $C = (\{0,1\}^\lambda)^2$. For each one:

1. Give the corresponding Dec algorithm.
2. State whether the scheme has CPA security. (Assume KeyGen samples the key uniformly from $\{0,1\}^\lambda$.) Among all those that have CPA security, pick one and give the security proof. For all those that are not secure, describe an adversary that breaks CPA-security.

(a)

$\mathsf{Enc}(k, m)$:
$r \leftarrow \{0,1\}^\lambda$
$z := F(k, m) \oplus r$
return (r, z)

(b)

$\mathsf{Enc}(k, m)$:
$r \leftarrow \{0,1\}^\lambda$
$s := r \oplus m$
$x := F(k, r)$
return (s, x)

(c)

$\underline{\mathsf{Enc}(k, m)\text{:}}$
$s_1 \leftarrow \{0,1\}^\lambda$
$s_2 := s_1 \oplus m$
$x := F(k, s_1)$
$y := F(k, s_2)$
return (x, y)

Hint: In all arguments and security proofs, you may use CPA- or CPA$-security and you may use the PRP switching lemma to start with the assumption that F is a PRF.

8.3 Modes of operation (3 pts)

Consider encryption with one of the CBC, OFB and CTR modes of operation and suppose one single bit in the ciphertext is changed. How does this influence the decryption of the ciphertext, that is, which decrypted plaintext blocks are affected by the error?