Applied Cryptography, FS2023
Apr 20–21, 2023 // Version 1.1

Exercise Sheet 8

Prof. Kenny Paterson, F. Günther
M. Backendal, M. Filić

Discussion Questions (Take-aways and public-key cryptography).

(a) We have finished the symmetric-key cryptography part of the course. What are your main take-aways from this part? What are the main applications of symmetric crypto, and what are the advantages and challenges of using it?

(b) For most of the second part of the course, we will discuss public-key cryptography, starting with this exercise sheet. What applications of public-key cryptography do you already know, and can you give an argument why these applications couldn't be solved using some of the symmetric-key primitives you've seen in the first part of the course?

Suggested focus. Attempt these problems
before class (if time): Problem 2.
in class: Problem 1.

Suggested reading. Reading the following sections in the Boneh-Shoup book [1] might help with the problems on this exercise sheet: Sections 9.2.2 and 9.2.3 (Implications of AE). Appendix A (number theory).

Problem 1 (Relations between security notions for symmetric encryption). By now, you have seen four security notions for symmetric encryption. Two for privacy: indistinguishability under chosen-plaintext attacks (IND-CPA) and indistinguishability under chosen-ciphertext attacks (IND-CCA), and two for integrity: integrity of plaintexts (INT-PTXT) and integrity of ciphertexts (INT-CTXT). In this exercise, we will study the relations between these notions.

(a) We begin by formalizing indistinguishability under chosen-ciphertext attack (IND-CCA). The game below (without code in boxes) recalls the IND-CPA definition. Fill in the missing code in the boxes of the dec oracle, such that the resulting game (with code in boxes included) defines IND-CCA. (Note that in the IND-CPA game, the adversary is not given oracle access to dec.)

```
Game $\textbf{IND-CPA}(\mathcal{A}, \mathrm{SE})$ $\boxed{\textbf{IND-CCA}(\mathcal{A}, \mathrm{SE})}$:
  $b \leftarrow\$ \{0,1\}$
  $\mathsf{K} \leftarrow\$ \mathrm{KGen}()$
  $\boxed{S \leftarrow \emptyset}$
  $b' \leftarrow\$ \mathcal{A}^{\mathsf{LoR}, \boxed{\mathsf{dec}}}()$
  Return $(b' = b)$

Oracle $\mathsf{LoR}(m_0, m_1)$:
  If $|m_0| \neq |m_1|$ then return $\perp$
  $c \leftarrow\$ \mathrm{Enc}(\mathsf{K}, m_b)$
  $\boxed{\qquad\qquad}$
  Return $c$

Oracle $\mathsf{dec}(c)$:
  $\boxed{\qquad\qquad}$
  $\boxed{\qquad\qquad}$
  $\boxed{\qquad\qquad}$
```

We define the advantange of an adversary $\mathcal{A}$ in the above games as:

$$\mathbf{Adv}_{\mathrm{SE}}^{\text{IND-CPA/CCA}}(\mathcal{A}) = 2 \cdot \left| \Pr\left[\,\text{Game } \textbf{IND-CPA/CCA}(\mathcal{A}, \mathrm{SE}) \Rightarrow \mathsf{true}\,\right] - \frac{1}{2} \right|.$$

(b) Argue informally why IND-CCA security implies IND-CPA security.

(c) Show that INT-CTXT is a strictly stronger notion than INT-PTXT (i.e., INT-CTXT $\implies$ INT-PTXT, but INT-PTXT $\not\Longrightarrow$ INT-CTXT).

1) INT-CTXT $\implies$ INT-PTXT. Argue briefly why INT-CTXT implies INT-PTXT, focusing on the winning conditions.

2) INT-PTXT $\not\Longrightarrow$ INT-CTXT. Complete the separation by providing a symmetric encryption scheme that is INT-PTXT secure, but not INT-CTXT secure. Show that the scheme is not INT-CTXT secure. Explain (informally) why the scheme is INT-PTXT secure. **Hint:** Use the approach used in Lectures 14–17, slide 17.

Let us now establish the most important relations among the mentioned notions. More precisely, we consider the (combinations of) notions shown in Figure 1.

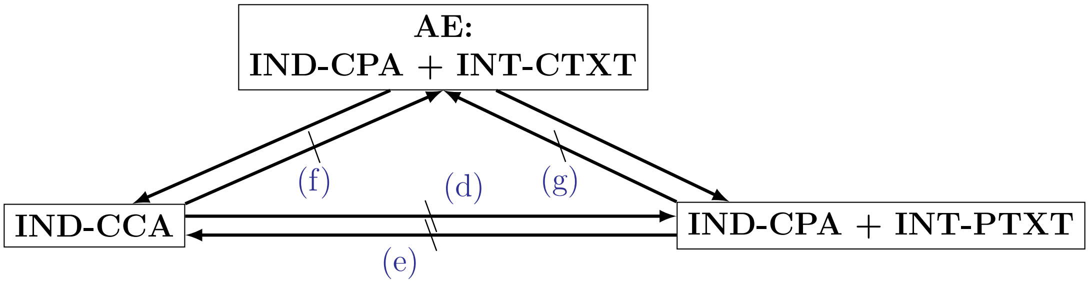

Figure 1: Relations among security notions: AE, IND-CPA + INT-PTXT, and IND-CCA.

We have already established that AE implies IND-CCA (Lectures 18–21, slides 20–26) and IND-CPA + INT-PTXT (since we showed that INT CTXT implies INT-PTXT in part (c) 1)).

(d) Show that IND-CCA $\not\Longrightarrow$ IND-CPA + INT-PTXT by showing that

$$\text{IND-CCA} \not\Longrightarrow \text{INT-PTXT}.$$

Start with an IND-CCA secure scheme $\mathrm{SE}_1 = (\mathrm{KGen}_1, \mathrm{Enc}_1, \mathrm{Dec}_1)$. Then

1) transform it into a scheme $\mathrm{SE}_1' = (\mathrm{KGen}_1, \mathrm{Enc}_1', \mathrm{Dec}_1')$,

2) show that SE_1' is still IND-CCA secure (providing a reduction),

3) but not INT-PTXT secure (providing an adversary).

Hint: Adapt your separation from part (c) 2), using the approach from Lectures 14–17, slide 17.

(e) Show that

$$\text{IND-CPA} + \text{INT-PTXT} \;\not\Longrightarrow\; \text{IND-CCA}.$$

Start with an IND-CPA and INT-PTXT secure scheme $\mathrm{SE}_2 = (\mathrm{KGen}_2, \mathrm{Enc}_2, \mathrm{Dec}_2)$ and

1) transform it into a scheme $\mathrm{SE}'_2 = (\mathrm{KGen}_2, \mathrm{Enc}'_2, \mathrm{Dec}'_2)$,
2) show that SE'_2 is still IND-CPA secure (providing a reduction)
3) and INT-PTXT secure (providing a reduction),
4) but not IND-CCA secure (providing an adversary).

(f) Explain why part (d) and established implications imply "IND-CCA $\not\Longrightarrow$ AE".

(g) Explain why part (e) and established implications imply "IND-CPA + INT-PTXT $\not\Longrightarrow$ AE".

(h) For this part (only), we slightly change the **INT-PTXT** and **INT-CTXT** games and allow *multiple* `try` queries. Show that this change does not substantially help the adversary to win these games. Let $\mathcal{A}_q$ be any adversary against the INT-CTXT security of a symmetric encryption scheme SE making q queries to its `try` oracle. Show that there exists an adversary $\mathcal{A}_1$ playing against the INT-CTXT security of SE and making only one query to its `try` oracle such that:

$$\mathbf{Adv}^{\text{INT-CTXT}}_{\text{SE}}(\mathcal{A}_1) \geq \frac{1}{q} \cdot \mathbf{Adv}^{\text{INT-CTXT}}_{\text{SE}}(\mathcal{A}_q).$$

Hint: Use an approach similar to the one used to show that AE implies IND-CCA security, specifically the part for the INT-CTXT reduction (Lectures 18–21, slides 20–26).

Explain (informally) why the same holds for INT-PTXT.

Problem 2 (Number theory refresher).

(a) (Integers modulo n) Given a positive integer n we define the set of integers modulo n to be the set with n elements:

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}.$$

The bars over the numbers are introduced to make a distinction between the usual integer, say $3 \in \mathbb{Z}$, and the elements in $\mathbb{Z}_n$, such as $\bar{3} \in \mathbb{Z}_n$.

We can perform sum, products, and differences in this set as follows: perform the operation as if the elements were integers, and compute the remainder of the resulting integer x when divided by n, i.e., $a \equiv x \bmod n$ (the modulus). The result of the operation is then an element $\bar{a} \in \mathbb{Z}_n$. The key point here is that for $a, b \in \mathbb{Z}$, $\bar{a} = \bar{b}$ if and only if $a \bmod n = b \bmod n$. $\bar{1}$ is a special element in $\mathbb{Z}_n$ called the multiplicative unity as it satisfies the following: for every $\bar{a} \in \mathbb{Z}_n$, $\bar{1} \cdot \bar{a} = \bar{a}$.

We say that $\bar{b}$ divides $\bar{a}$ in $\mathbb{Z}_n$ if there exists $\bar{k} \in \mathbb{Z}_n$ such that $\bar{a} = \bar{b} \cdot \bar{k} \mod n$. The divisors of $\bar{1}$ are called *units*. The set of all units in $\mathbb{Z}_n$ is denoted with $\mathbb{Z}_n^*$. For every $\bar{a}, \bar{b} \in \mathbb{Z}_n$ such that $\bar{a} \cdot \bar{b} = \bar{1}$ we say that $\bar{a}$ is the multiplicative inverse of $\bar{b}$, and $\bar{b}$ is the multiplicative inverse of $\bar{a}$. By definition, every element in $\mathbb{Z}_n^*$ has an inverse.

1) For calculating multiplicative inverses of elements in $\mathbb{Z}_n$, one can use the extended Euclidean algorithm (EEA). In general, given $a, b \in \mathbb{Z}$, EEA calculates $x, y, d \in \mathbb{Z}$ such that $ay + bx = d = \gcd(a, b)$ defining r_i, q_i, s_i, t_i sequences as follows.

$r_0 = a$	$r_1 = b$	$r_{i+1} = r_{i-1} - q_i \cdot r_i$
$s_0 = 1$	$s_1 = 0$	$s_{i+1} = s_{i-1} - q_i \cdot s_i$
$t_0 = 0$	$t_1 = 1$	$t_{i+1} = t_{i-1} - q_i \cdot t_i$
	$q_1 = \lfloor \frac{r_0}{r_1} \rfloor$	$q_i = \lfloor \frac{r_{i-1}}{r_i} \rfloor$

The computation stops when $r_{k+1} = 0$ for some iteration k. Then:

$$r_k = \gcd(a, b) = d, \qquad s_k = y, \qquad \text{and} \qquad t_k = x.$$

i. Solve $22 \cdot y + 7 \cdot x = 1$ using EEA.

ii. Find a multiplicative inverse of $\overline{111}$ in $\mathbb{Z}^*_{1001}$, i.e. find $\overline{x}$ such that $111x \equiv 1 \bmod 1001$.

2) In general, the EEA computes coefficients of what is called Bézout's identity: For $a, b \in \mathbb{Z}$ and $\gcd(a, b) = d$ there exist integers $y, x \in \mathbb{Z}$ such that

$$ya + xb = d.$$

However, for $d = 1$ (a and b are coprime), even a stronger claim holds: *Let $a, b \in \mathbb{Z}$. Then, $\gcd(a, b) = 1$, if and only if, there exist integers $y, x \in \mathbb{Z}$ such that $ya + xb = 1$.* Prove this claim.

3) Show that $\bar{k} \in \mathbb{Z}_n$ is a unit, if and only if, $\gcd(n, k) = 1$.

Hint: You may want to use claim 2).

4) Show that if $\bar{a}, \bar{b} \in \mathbb{Z}^*_n$ then $\bar{a} \cdot \bar{b} \in \mathbb{Z}^*_n$.

5) Let $\bar{k} \in \mathbb{Z}^*_n$ and $\bar{a}, \bar{b} \in \mathbb{Z}^*_n$. Show that $\bar{a} = \bar{b}$, if and only if, $\bar{k} \cdot \bar{a} = \bar{k} \cdot \bar{b}$.

6) Given a positive integer n, show that the Euler's totient function of n, $\phi(n)$, can be calculated in terms of elements from $\mathbb{Z}_n$.

(Euler's totient function counts the positive integers up to a given integer n that are relatively prime to n.) **Hint:** You may want to use claim 3).

7) Show that if $\bar{k} \in \mathbb{Z}^*_n$, then $\bar{k}^{\phi(n)} = \bar{1}$. **Hint:** You may want to use claims 4), 5) and 6).

8) By the definition at the beginning of this problem and claim 4), one can see that $\mathbb{Z}^*_n$, together with multiplication, forms a group. We denote this group with $(\mathbb{Z}^*_n, \cdot)$, and sometimes refer to it as the multiplicative group modulo n. When n is prime, then $(\mathbb{Z}^*_n, \cdot)$ is isomorphic to $(\mathbb{Z}_{n-1}, +)$, written $(\mathbb{Z}^*_n, \cdot) \approxeq (\mathbb{Z}_{n-1}, +)$. Every element in a group has its order which is defined as follows. Let $g \in (\mathbb{G}, \cdot)$, then the order of g is defined as the minimum positive integer ℓ such that $g^\ell = 1_{\mathbb{G}}$. Note that isomorphic groups have the same number of elements of the same order.

Show that the number of elements of order 5 in the group $(\mathbb{Z}^*_{31}, \cdot)$ is 4.

(b) (Chinese Remainder Theorem)

The Chinese Remainder Theorem (CRT) [2] states the following:

Theorem 1. *Let $m_1, m_2, \dots, m_r$ be pairwise relative prime numbers, let $a_1, a_2, \dots a_r$ be integers. Then a system of congruences*

$$x \equiv a_1 \bmod m_1, \quad x \equiv a_2 \bmod m_2, \quad \dots \quad x \equiv a_r \bmod m_r$$

has a solution $x_0 = n_1x_1 + n_2x_2 + \dots + n_rx_r$ where $m := m_1m_2 \dots m_r$, $n_j := \frac{m}{m_j}$, and x_j is an integer such that $n_jx_j \equiv a_j \bmod m_j$.

Now solve the following system of congruences using the CRT.

$$x \equiv 3 \bmod 10, \quad x \equiv 8 \bmod 15, \quad x \equiv 5 \bmod 84. \tag{1}$$

Acknowledgements. This exercise sheet is in part inspired by (and adapted from) problems from the book “A Graduate Course in Applied Cryptography” by Dan Boneh and Victor Shoup and the book “Number Theory” by Andrej Dujella.

References

[1] D. Boneh and V. Shoup. *A Graduate Course in Applied Cryptography*. Online, version 0.6 edition, Jan. 2023.

[2] Chinese remainder theorem. https://www.cut-the-knot.org/blue/chinese.shtml.