Applied Cryptography, FS2023
April 27–28, 2023 // Version 1

Exercise Sheet 9

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

Discussion Questions (PKE key distribution and malleability).

(a) As put in the lectures:

> *At a high level, public-key encryption translates the problem of symmetric key distribution into the problem of distribution of authentic public keys.*

Is that an easier problem? How would you solve it? Do you know how it's solved in practice?

(b) You have seen Textbook RSA as a concrete PKE example. Given (only) the encryption $c = m^e \mod N$ of a message $m \in [1, N-1]$ and the public key (e, N), how can you obtain an encryption of the message $s \cdot m \mod N$ for some $s \in [1, N-1]$ of your choice? Is this malleability of ciphertexts good or bad?

Suggested focus. Attempt these problems
before class: Problem 1.
in class: Problem 2, Problem 3.

Suggested reading. Reading the following sections in the Boneh-Shoup book [2] might help with the problems on this exercise sheet: Sections 10.3 (for RSA basics) and Appendix A (for number theory). We assume that you are familiar with the extended Euclidean algorithm to compute GCD, with the Chinese Remainder Theorem (CRT), and with the square-and-multiply technique for fast modular exponentiation.

Problem 1 (Textbook RSA).
In this problem we explore various aspects of RSA encryption.

(a) An RSA user has a modulus $N = 91$ and an encryption key $e = 25$. Compute the following values by hand.

1) Find the decryption key d.
2) For the plaintext $m = 16$, compute the corresponding (Textbook RSA) ciphertext.

(b) Suppose that two users share the same RSA modulus N. In other words, user A has public key (N, e_A), and user B has public key (N, e_B). Obviously, A and B know the factorization of N so they can decrypt each other's messages. However, there is another reason why this is a bad situation.

Show that if a user encrypts the same message m to A and B and if $\gcd(e_A, e_B) = 1$ then an eavesdropper can calculate m given the ciphertexts c_A and c_B.

(c) The RSA encryption process is fast if the exponent e is very small. Let us explore the requirements and implications for choosing a very small value for e.

1) Show that $e = 2$ cannot be used as an RSA public exponent.

2) We can use $e = 3$ as an RSA public exponent. But what is the corresponding restriction on the prime factors of N?

3) Let $(N_1, 3)$, $(N_2, 3)$ and $(N_3, 3)$ be three distinct RSA public keys all with public exponent 3. Suppose a message m is encrypted and sent to all three users. Show that an eavesdropper can recover the message.

(d) One way to speed up RSA decryption would be to perform the following key generation method. First, choose two random large primes p and q and set $N = p \cdot q$. Next, choose two "very small" integers d_p, d_q (coprime to $p - 1$ and $q - 1$ respectively) such that

$$d_p \equiv d_q \mod \gcd(p-1, q-1).$$

Then use the Chinese Remainder Theorem to find an integer e such that

$$e \cdot d_p \equiv 1 \mod (p-1),$$

and

$$e \cdot d_q \equiv 1 \mod (q-1).$$

1) Describe how RSA decryption proceeds in this case. Also discuss the relative costs of encryption and decryption of this approach compared with textbook RSA with the standard choice of d.

2) Discuss the security of this revised system. In particular, is there an attack which works if the numbers d_p and d_q are too small?

Above we discussed a couple of attacks against RSA. Note that many more interesting attacks are summarized in a survey paper "Twenty Years of Attacks on the RSA Cryptosystem" by Dan Boneh [1].

Problem 2 (Constructing a KEM from a PKE scheme). Let $\mathsf{PKE} = (\mathrm{KGen}, \mathrm{Enc}, \mathrm{Dec})$ be a one-time IND-CPA secure PKE scheme with message space $\mathcal{M}$. Here, "one-time IND-CPA security" means that the IND-CPA game corresponding to PKE only allows at most a single left-or-right encryption query. From PKE we can construct a KEM $\mathsf{KEM} = (\mathrm{KGen}, \mathrm{Encap}, \mathrm{Dec})$ as follows. The key-generation and decapsulation algorithms of KEM are identical to the KGen resp. Dec algorithm of PKE. So we only describe the encapsulation algorithm Encap below.

```
$\mathrm{Encap}(pk)$
$K \leftarrow_{\$} \mathcal{M}$
$c \leftarrow \mathrm{Enc}(pk, K)$
Return $(c, K)$
```

Show that KEM is IND-CPA secure. The IND-CPA security game for KEMs is the IND-CCA security game from the lecture *without* the decapsulation oracle.

Problem 3 (Paillier PKE). In this exercise, we will be working with the Paillier public-key encryption scheme.

Given an RSA modulus $N = pq$, where p and q are distinct ℓ-bit primes (i.e., of same length) for $\ell > 2$, the scheme utilizes the group $\mathbb{Z}^*_{N^2}$. Recall that $\mathbb{Z}^*_n$ is a group closed under multiplication modulo n that consists of the set of positive integers $\{a \mid 1 \leq a < n \text{ and } gcd(a, n) = 1\}$.

(a) What is the order of the group $\mathbb{Z}^*_{N^2}$ (i.e., $|\mathbb{Z}^*_{N^2}|$) in terms of p and q?
Hint: Consider the potential divisors of a *and* N^2.

The Paillier key generation and encryption algorithms work as follows:

KGen(1^ℓ): Generate two distinct random ℓ-bit primes ($\ell > 2$) p and q. Let $N = pq$ and $d = (p-1)(q-1)$. Define the public key as $pk = N$ and secret key as $sk = d$. Output (pk, sk).

Enc(pk, m): Given public key $pk = N$ and message $m \in \{0, 1, \ldots, N-1\}$, choose uniformly at random $r \leftarrow_\$ \mathbb{Z}^*_{N^2}$. The corresponding ciphertext is then computed as $c = (1+N)^m r^N \mod N^2$.

(b) Show that $gcd(d, N) = 1$.

(c) For any integer $0 \leq a < N$, show that $(1+N)^a \equiv 1 + aN \mod N^2$. What happens when $a = N$? **Hint:** Use binomial expansion.

(d) Using the parts (a) and (c), describe a decryption algorithm Dec and prove the correctness of the final Paillier PKE scheme (KGen, Enc, Dec). **Hint:** Start with $c^d \mod N^2$ and try to recover m.

(e) Show that the Paillier scheme is *additively homomorphic*: For ciphertexts $c_0 \leftarrow \text{Enc}(pk, m_0)$ and $c_1 \leftarrow \text{Enc}(pk, m_1)$ of messages $m_0, m_1 \in \{0, 1, \ldots, N-1\}$, show that for a new ciphertext $c = c_0 \cdot c_1 \mod N^2$, $\text{Dec}(sk, c) = (m_0 + m_1) \mod N$.

(f) Is the Paillier scheme IND-CCA secure? **Hint:** Consider what the additive homomorphism entails.

Acknowledgements. This exercise sheet is in part inspired by (and adapted from) problems by Siaw-Lynn Ng and Simon Blackburn, as well as the books “A Graduate Course in Applied Cryptography” by Dan Boneh and Victor Shoup, and “Introduction to Modern Cryptography” by Jonathan Katz and Yehuda Lindell.

References

[1] D. Boneh et al. Twenty years of attacks on the rsa cryptosystem. *Notices of the AMS*, 46(2):203–213, 1999.

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