6.875: Cryptography and Cryptanalysis **October 6, 2021**

Last updated: October 7, 2021

Problem Set 3

Instructor: Vinod Vaikuntanathan

TAs: Lali Devadas, Aparna Gupte, Sacha Servan-Schreiber

Instructions.

- **When:** This problem set is due on **October 20, 2021** before **11pm ET**.
- **How:** You should use LaTeX to type up your solutions (you can use our LaTeX template from the course webpage). Solutions should be uploaded on Gradescope as a single pdf file.
- **Acknowledge your collaborators:** Collaboration is permitted and encouraged in small groups of at most three. You must write up your solutions *entirely on your own* and *acknowledge your collaborators*.
- **Reference your sources:** If you use material from outside the lectures, you must reference your sources (papers, websites, wikipedia, ...).
- **When in doubt, ask questions:** Use Piazza or the TA office hours for questions about the problem set. See the course webpage for the timings.

Problem 1. Find the one-way function! Almost all cryptographic primitives imply the existence of a one-way function. In this problem, you will prove that both public key and secret key encryption imply the existence of a one-way function.

> **For each of the following cryptographic primitives: assuming you have an arbitrary scheme $\mathcal{E}$ which satisfies perfect correctness and the security definition, construct a one-way function based on $\mathcal{E}$, and prove its one-wayness.**

(a) IND-CPA-secure *public key* encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

(b) IND-CPA-secure *secret key* encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

The syntax of the above schemes:

Public key encryption

- $(sk, pk) \leftarrow \mathsf{Gen}(1^\lambda)$
- $c \leftarrow \mathsf{Enc}(pk, sk, m \in \mathcal{M})$
- $m \leftarrow \mathsf{Dec}(sk, c)$

Secret key encryption

- $sk \leftarrow \mathsf{Gen}(1^\lambda)$
- $c \leftarrow \mathsf{Enc}(sk, m \in \mathcal{M})$
- $m \leftarrow \mathsf{Dec}(sk, c)$

Problem 2. Validating RSA ciphertexts

Alice is a stock broker communicating with the New York Stock Exchange (NYSE). To prevent a competing trader Eve from learning whether she is issuing BUY or SELL orders to NYSE, all communication to NYSE is encrypted using the RSA scheme described in Figure 1, where NYSE holds the secret key. The messages BUY ($m = 0$) and SELL ($m = 1$) are encoded as a bit which only NYSE can recover using the secret key.

The encryption scheme described below relies on the RSA assumption and uses the fact that the least significant bit (LSB) of an RSA encryption is a hardcore bit.

$\mathsf{Gen}(1^\lambda)$

1 : sample random distinct
2 : λ-bit primes p and q
3 : $N := pq$
4 : $e \xleftarrow{R} \mathbb{Z}_N^*,\ d := e^{-1} \pmod{\phi(N)}$
5 : $sk := d,\ pk := (N, e)$
6 : **return** (sk, pk)

$\mathsf{Enc}(pk, m \in \{0,1\})$

1 : **parse** $pk = (N, e)$
2 : $r \xleftarrow{R} \{1, 2, \ldots, 2^{\lambda-1} - 1\}$
3 : $c := (2r + m)^e \pmod{N}$
4 : **return** c

$\mathsf{Dec}(pk, sk, c)$

1 : **parse** $pk = (N, e)$ and $sk = d$
2 : $\tilde{c} := c^d \pmod{N}$
3 : **return** $\mathsf{LSB}(\tilde{c})$

Figure 1: The RSA scheme

Corrupted ciphertexts. However, because Alice is forced to use Xfinity (which has notoriously faulty connections), ciphertexts aren't always reliably transmitted to NYSE: some bits of the ciphertexts are flipped with high probability. However, such corruption is *undetectable* by NYSE, who will happily decrypt an (invalid) message from the corrupted ciphertext, e.g., potentially recovering SELL when Alice sent BUY. To prevent the NYSE from recovering an incorrect message when a ciphertext is corrupted, Alice proposes a variant of the RSA scheme with an integrated "message validity check", described in Figure 3. If any bits of the ciphertext c are corrupted (i.e., flipped) before being received by the NYSE, then the goal is to ensure that $\mathsf{Dec}(pk, sk, c) = \perp$ (the decryption fails) with overwhelming probability, and NYSE responds by asking the sender to re-transmit her message. Alice's scheme ensures that all valid encryptions have the same format (visualized in Figure 2).

Figure 2: Bit-wise representation of a message encrypted using Alice's variant of the RSA scheme. The randomness is added to make each ciphertext look random while the zeroes are added to detect corruption with high probability; the least significant bit m encodes the BUY or SELL action.

Suppose Eve intercepts an encryption of m under the RSA scheme of Figure 3 sent by Alice before it is corrupted (perhaps she has access to Alice's WiFi router). Provide an attack showing that Eve can recover the message bit m (encoding BUY or SELL) by interacting with the NYSE. *You may assume that Eve has a perfect internet connection with the NYSE (ciphertexts are never corrupted when sent to NYSE by Eve).*

$\mathsf{Gen}(1^\lambda)$

1 : sample random distinct
2 : λ-bit primes p and q
3 : $N := pq$
4 : $e \xleftarrow{R} \mathbb{Z}_N^*,\ d := e^{-1} \pmod{\phi(N)}$
5 : $sk := d,\ pk := (N, e)$
6 : **return** (sk, pk)

$\mathsf{Enc}(pk, m \in \{0,1\})$

1 : **parse** $pk = (N, e)$
2 : $r \xleftarrow{R} \{1, 2, \ldots, 2^{\lambda-1} - 1\}$
3 : $c := (2^\lambda r + m)^e \pmod{N}$
4 : **return** c

$\mathsf{Dec}(pk, sk, c)$

1 : **parse** $pk = (N, e)$ and $sk = d$
2 : $\tilde{c} := c^d \pmod{N}$
3 : `// change to bit representation`
4 : $t := \tilde{c}_1 \ldots \tilde{c}_\ell$ `// (LSB is` $\tilde{c}_\ell$`)`
5 : **if** $\ell < \lambda + 1$: **return** $\perp$
6 : **if** $t_{[\ell-\lambda+1:\ell-1]} \neq 0^{\lambda-1}$: **return** $\perp$
7 : **else** : **return** $\mathsf{LSB}(\tilde{c})$

Figure 3: Alice's RSA scheme with integrated message validity checking

Problem 3. A simpler variant of AES encryption?

The Advanced Encryption Standard (AES) is a block cipher that encrypts messages in rounds (typically $r = 10$) using a series of random round keys $k_1, \ldots, k_r$ and a deterministic round function R. At a high level, when encrypting a message using AES, the input to round 1 is the message and the input to the round function R at round i is the output of R from round $i - 1$. The round function is deterministic and permutes the input using the random round key k_i. Using the keys $k_1, \ldots, k_r$, it is possible to "unroll" each round and recover the original message (i.e., using the keys it is possible to decrypt and recover the message). However, without knowledge of the round keys, it is conjectured that AES is a pseudo-random permutation. In this problem we will explore a simpler version of the same idea; your job will be to break it.

Consider the following simplification of AES encryption with keys $k_1, \ldots, k_r$ (r is the number of rounds). Define the following *round function* $R(k_i, x) = x^{-1} + k_i \bmod p$ where p is some large prime (e.g., p is a 128 bit prime). Note that R is public and known to everyone; only the random round keys are kept secret. Define the function $F(k_1, \ldots, k_r, x)$ to output R evaluated iteratively for r rounds (using the round key k_i for round i). That is, on input $(k_1, \ldots, k_r, x)$, set

$$\begin{aligned} x_1 &\leftarrow R(k_1, x), \\ x_2 &\leftarrow R(k_2, x_1), \\ x_3 &\leftarrow R(k_3, x_2), \\ &\ldots, \\ x_r &\leftarrow R(k_r, x_{r-1}), \end{aligned}$$

and output $F(k_1, \ldots, k_r, x) = x_r$.

(a) **Show that F is a permutation. That is, there exists a function F^{-1} such that $F^{-1}(k_1, \ldots, k_r, F(k_1, \ldots, k_r, x)) = x$.**

(b) **Provide an attack breaking this toy version of AES. That is, show that F is not a pseudo-random permutation. (Hint: in fact, given $F(k_1, \ldots, k_r, x)$, $F(k_1, \ldots, k_r, y)$, $F(k_1, \ldots, k_r, z)$ for three inputs x, y, z, you can compute $F(k_1, \ldots, k_r, w)$ for any w.)**

Problem 4. Circular security

Alice has an arbitrary public key encryption scheme where the messages and keys are strings in $\{0,1\}^\lambda$. Alice generates her keys pk and sk and stores them on her hard drive. Alice then encrypts the whole hard drive using her public key pk. An attacker gains access to the encrypted contents of her hard-drive. Can you argue that her data is still secure? Formally,

Definition 1 (Circular Security)**.** *A public key encryption scheme* $\mathsf{PKE} = (\mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ *with message space* $\mathcal{M} = \mathcal{K}$ *is said to be circular secure if for all PPT* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$*, there exists a negligible function* $\mathsf{negl}(\lambda)$ *such that:*

$$\Pr\left[\begin{array}{l}(pk, sk) \leftarrow \mathsf{PKE.Gen}(1^\lambda);\ c^* \leftarrow \mathsf{PKE.Enc}(pk, sk);\\ (m_0, m_1, \mathsf{state}) \leftarrow \mathcal{A}_1(pk, c^*);\\ b \xleftarrow{R} \{0,1\};\ c_b \leftarrow \mathsf{PKE.Enc}(pk, m_b);\\ b' \leftarrow \mathcal{A}_2(pk, c_b, \mathsf{state}) :\\ b' = b\end{array}\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda).$$

Does every IND-CPA encryption scheme satisfy Definition 1? Either provide a proof showing all IND-CPA-secure public key encryption schemes satisfy Definition 1 or provide a counterexample.

Problem 5. Digital signatures from RSA

Alice wants to use the RSA digital signature scheme defined as follows:

$\mathsf{Gen}(1^\lambda)$

1: sample random distinct
2: λ-bit primes p and q
3: $p' \leftarrow p^{-1} \pmod q$
4: $q' \leftarrow q^{-1} \pmod p$
5: $N \leftarrow pq$
6: $e \xleftarrow{R} \mathbb{Z}_N^*,\ d \leftarrow e^{-1} \pmod{\phi(N)}$
7: $sk := (d, p, q, p', q'),\ pk := (N, e)$
8: **return** (sk, pk)

$\mathsf{Sign}(pk, sk, m \in \mathcal{M})$

1: **parse** $pk = (N, e)$
2: and $sk = (d, p, q, p', q')$
3: $\sigma_p \leftarrow m^d \pmod p$
4: $\sigma_q \leftarrow m^d \pmod q$
5: $\sigma \leftarrow \sigma_p q q' + \sigma_q p p' \pmod N$
6: **return** σ

$\mathsf{Verify}(pk, m, \sigma)$

1: **parse** $pk = (N, e)$
2: **if** $\sigma^e = m \pmod N$:
3: **return** 1
4: **else** : **return** 0

Note that in Sign*, the signature is computed by applying the Chinese remainder theorem. This is done so as to make the signature algorithm more efficient as it results in two exponentiations modulo a λ-bit number (and one addition mod N) rather than a single exponentiation mod N. This does not compromise security and is a standard way of improving efficiency in practice.*

Unfortunately, the part of Alice's computer responsible for modular exponentiation is being affected by cosmic radiation, so anytime she computes a signature, each bit of σ_p and each bit of σ_q is flipped with probability $\frac{1}{\lambda}$. (Yes, this is a real phenomenon.[1]) The computation of σ from σ_p and σ_q is unaffected by radiation.

Given the problems with Alice's computer, show that she cannot expect security of this signature scheme to hold. That is, provide an attack on the EUF-CMA security of this scheme, noting that the Sign oracle in the EUF-CMA security game will suffer from the bit-flipping described above.

[1] https://www.wnycstudios.org/podcasts/radiolab/articles/bit-flip

Problem 6. Fun with collision-resistant hash functions

A hash function family $\mathcal{H}$ is a pair of algorithms $(\mathsf{Gen}, \{h_k\}_k)$ where:

1. $\mathsf{Gen}(1^\lambda)$ is an efficient randomized algorithm that outputs a key k.
2. $h_k : \{0,1\}^* \to \{0,1\}^\lambda$ is an efficient algorithm parameterized by key k that compresses arbitrary length strings to λ-bit strings.

A collision-resistant hash function (CRHF) is defined as follows.

Definition 2 (Collision-resistant hash function)**.** *A hash function family $\mathcal{H} = (\mathsf{Gen}, \{h_k\}_k)$ is said to be collision-resistant if for all PPT adversaries $\mathcal{A}$ there exists a negligible function $\mathsf{negl}(\cdot)$ such that:*

$$\Pr\left[\begin{array}{l} k \leftarrow \mathsf{Gen}(1^\lambda); \\ (x, x') \leftarrow \mathcal{A}(1^\lambda, k, \mathcal{H}) : x \neq x' \wedge h_k(x) = h_k(x') \end{array}\right] \leq \mathsf{negl}(\lambda).$$

That is, an adversary $\mathcal{A}$ that is given the hash function *and key* cannot generate a collision (i.e., two values $x \neq x'$ such that $h_k(x) = h_k(x')$) except with negligible probability $\mathsf{negl}(\lambda)$.

Let $\mathcal{H}_1 = (\mathsf{Gen}_1, \{h^1_k\}_k)$ and $\mathcal{H}_2 = (\mathsf{Gen}_2, \{h^2_k\}_k)$ be two CRHF families. Define $\mathsf{Gen}'(1^\lambda)$ to return (k_1, k_2) where $k_1 \leftarrow \mathsf{Gen}_1(1^\lambda), k_2 \leftarrow \mathsf{Gen}_2(1^\lambda)$. For each of the following, either prove that $\mathcal{H}' = \left(\mathsf{Gen}', \{h'_{k_1,k_2}\}_{k_1,k_2}\right)$ is a CRHF family or provide a counterexample showing that it is not always collision-resistant.

(a) $h'_{k_1,k_2}(x) = h^1_{k_1}(x) \,||\, h^2_{k_2}(x)$

(b) $h'_{k_1,k_2}(x) = h^1_{k_1}(h^2_{k_2}(x))$