Exercise Sheet 13

Cryptography and Security 2025

Exercise 1 A Bad EKE with RSA

In this exercise we want to apply the EKE construction with the RSA cryptosystem and the AES cipher to derive a password-based authenticated key exchange protocol (PAKE). For that, Alice and Bob are assumed to share a (low-entropy) password w. The protocol runs as follows:

Alice password: w		**Bob** password: w
$\mathsf{RSAGen} \to (\mathsf{sk}, N)$, $B_1 \| \cdots \| B_8 \leftarrow N$		
$C_1 \| \cdots \| C_8 \leftarrow \mathsf{AESCBC}_w(B_1 \| \cdots \| B_8)$	$\xrightarrow{C_1 \| \ldots \| C_8}$	$B_1 \| \cdots \| B_8 \leftarrow \mathsf{AESCBC}_w^{-1}(C_1 \| \cdots \| C_8)$
		$N \leftarrow B_1 \| \cdots \| B_8$, pick $K \in \{0,1\}^{128}$
		$\Gamma \leftarrow \mathsf{RSAEnc}_{N,3}(K)$, $B'_1 \| \cdots \| B'_8 \leftarrow \Gamma$
$B'_1 \| \cdots \| B'_8 \leftarrow \mathsf{AESCBC}_w^{-1}(C'_1 \| \cdots \| C'_8)$	$\xleftarrow{C'_1 \| \cdots \| C'_8}$	$C'_1 \| \cdots \| C'_8 \leftarrow \mathsf{AESCBC}_w(B'_1 \| \cdots \| B'_8)$
$\Gamma \leftarrow B'_1 \| \cdots \| B'_8$, $K \leftarrow \mathsf{RSADec}_{\mathsf{sk}}(\Gamma)$		
output: K		output: K

Here are some explanations:

- Alice generates an RSA modulus N such that $\gcd(3, \varphi(N)) = 1$. This modulus is supposed to have exactly 1024 bits. The modulus N is written in binary and splits into 8 blocks $N = B_1 \| \cdots \| B_8$. The blocks $B_1, \ldots, B_8$ are then encrypted with AES in CBC mode with IV set to the zero block and the key set to w. The obtained ciphertext blocks $C_1, \ldots, C_8$ are sent to Bob.
- Bob decrypts $C_1, \ldots, C_8$ following the AES-CBC decryption algorithm with IV set to the zero block and the key set to w. He recovers $B_1, \ldots, B_8$ and can reconstruct N. He picks a random 128-bit key K and computes the RSA-OAEP encryption of K with key N and $e = 3$. He then obtains a ciphertext Γ. This is split into 8 blocks $\Gamma = B'_1 \| \cdots \| B'_8$ and the blocks $B'_1, \ldots, B'_8$ are then encrypted with AES in CBC mode with IV set to the zero block and the key set to w. The obtained ciphertext blocks $C'_1, \ldots, C'_8$ are sent to Alice.
- Alice decrypts $C'_1, \ldots, C'_8$ following the AES-CBC decryption algorithm with IV set to the zero block and the key set to w. She recovers $B'_1, \ldots, B'_8$ and can reconstruct Γ. She applies the RSA-OAEP decryption on Γ with her secret key and obtains K.

So, Alice and Bob end the protocol with the secret K.

1. Assume (*only in this question*) that we use plain RSA instead of RSA-OAEP. Show that Eve can easily recover w and K in a *passive* attack with a single execution of the protocol.

   HINT: show that the plain RSA decryption of Γ is easy in this case.

2. Propose a *passive* attack allowing Eve to deduce the password w after a few executions of the protocol. Estimate the number of executions needed to recover a password with less than 48 bits of entropy with a high probability.

   HINT: N is not an arbitrary bitstring. You could think of eliminating some password guesses.

Exercise 2 Reset Password Recovery

We consider a non-uniform distribution D of passwords. Passwords are taken from a set $\{k_1, \ldots, k_n\}$ and each password k_i is selected with probability $\Pr_D[k_i]$. (We omit the subscript D when there is no ambiguity in the distribution.) For simplicity, we assume that $\Pr[k_1] \geq \Pr[k_2] \geq \cdots \geq \Pr[k_n]$. We consider a game in which a cryptographer apprentice plays with a black-box device which has two buttons — a *reset* button and a *test* button — and a keyboard.

- When the player pushes the reset button, the device picks a new password K, following the above distribution, and stores it into its memory. The game cannot start before the player pushes this button.
- The player can enter an input w on the keyboard and push the test button. This makes the device compare K with w. If $K = w$, the device opens, the player wins, and the game stops. Otherwise, the device remains closed and the player continues.

A strategy is an algorithm that the player follows to play the game. Given a strategy, we let C denote the expected number of times the player pushes the test button until he wins. The goal of the player is to design a strategy which uses a minimal C.

In this exercise, we consider several strategies. To compare them, we use a toy distribution T defined by the parameters a, p and

$$\Pr_T[k_1] = \cdots = \Pr_T[k_a] = \frac{p}{a} \quad , \quad \Pr_T[k_{a+1}] = \cdots = \Pr_T[k_n] = \frac{1-p}{n-a}$$

and assuming that $\frac{p}{a} \geq \frac{1-p}{n-a}$.

1. We consider a strategy in which the player always pushes the reset button before pushing the test button. For a general distribution D, give an optimal strategy and the corresponding value of C.

   Apply the general result to the toy distribution T.

2. We consider a strategy in which the reset button is never used again after the initial reset. For a general distribution D, give an optimal strategy and the corresponding value of C.

   Apply the general result to the toy distribution T.

3. For $n = 3$ and $a = 1$, propose one value for p in the toy distribution T so that the strategy in 2 is better and one value for p so that the strategy in 1 is better.

   We recall that we must have $\frac{p}{a} \geq \frac{1-p}{n-a}$.

4. We consider a strategy in which the player always pushes the reset button after m tests have been made since the last reset. For a general distribution D, give an optimal strategy and the corresponding value of C.

   Check that your result is consistent with those from 1 and 2 with $m = 1$ and $m = n$.