Cryptography – Homework 6

Discussed on 06.02.2019.

Exercise 6.1 RSA

For this exercise we will use the notation (for elements of the RSA-PKES and PSS$[k,l]$) introduced in the lecture. We will use msbf-representation throughout the exercise.

(a) We choose two primes $p = 17$ and $q = 19$, select $e = 5$ and use them for instantiating the RSA encryption scheme. Then $N = pq = 323 = (101000011)_2$ in MSBF, i.e., N's bit-length is 9. We apply the OAEP padding scheme to the messages we want to encrypt using the following (very simple and unrealistic) instantiation:

- (Unpadded) messages m are 3-bit strings,
- $k_1 = 2$ and $k_0 = 4$,
- $G(x_1x_2x_3x_4) = x_1x_2x_3x_4x_1$, for $x_i \in \{0,1\}$ for $1 \leq i \leq 4$,
- $H(x_1x_2x_3x_4x_5) = (x_1 \oplus x_2)(x_2 \oplus x_3)(x_3 \oplus x_4)(x_4 \oplus x_5)$, for $x_i \in \{0,1\}$ for $1 \leq i \leq 5$.

Let us assume we receive the ciphertext 116. Compute d and the original (3-bit) message. Apply the Chinese Remainder Theorem in your computation.

(b) Show that decoding/encoding works regardless of the choice for G and H in the OAEP padding scheme.

(c) We assumed for the RSA scheme that the plaintext message m is an element of $\mathbb{Z}_N^*$. Show that encryption and decryption is also possible if $m \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$.

(d) We want to sign a message using the PSS$[k,l]$ scheme. We reuse the values from the previous exercise for N, d and e, and add the following parameters:

- $n = 10$, $k = l = 3$,
- $h(x_1 \dots x_s) := x_1x_2x_3$,
- $g(x_1x_2x_3) := x_1x_2x_3x_1x_2x_3$.

Compute $\mathsf{Sgn}_{(323,d)}(0110)$. Assume hereby that r was chosen as the bitstring 101.

Exercise 6.2 Attacks on Textbook-RSA

In this exercise we will study Textbook-RSA and see why it is insecure and why we have to use a variant with random padding in practice.

(a) Suppose $e = 3$ and Alice sends the same message m encrypted to three (or more) different persons having RSA-keys $(N_1, e), (N_2, e), (N_3, e)$. Show how Eve can compute m having only eavesdropped the three ciphertexts c_1, c_2, c_3.

(b) Suppose we want to use Textbook-RSA in a hybrid encryption choosing large enough primes such that $N > 2^{1024}$ and $e = 7$. We want to encrypt AES-keys, i.e. messages from $\{0,1\}^{128}$. Explain why this is a really bad idea!

Exercise 6.3 Elgamal PKES—why to work in $\mathbb{QR}_p$

Construct a CPA-attack on Elgamal relative to $\mathsf{Gen}\mathbb{Z}^*_{\text{safe}}$, i.e. Gen returns

$$I = (\langle \mathbb{Z}_p^*, 1, \cdot \rangle, q, g, x, h)$$

with p a n-bit prime, $q = p - 1$, and g generates all elements in $\mathbb{Z}_p^*$.)
Hint: Consider the observations made about the DDH problem relative to $\mathsf{Gen}\mathbb{Z}^*_{safe}$ *in the lecture.*

Exercise 6.4 Elgamal's DSS—why it fails without hashing

Elgamal already showed in his paper, how to efficiently forge a valid tag for a new message:

- Let (m, r, s) be a valid message-tag pair.
- Choose $A, B, C \in \mathbb{Z}$ s.t. $\mathsf{gcd}(Ar - Cs, p - 1) = 1$.
- Set $r' := r^A \cdot g^B \cdot y^C \bmod p$, $s' := sr'(Ar - Cs)^{-1} \bmod p - 1$, and $m' := r'(Am + Bs)(Ar - Cs)^{-1} \bmod p - 1$.

Show that (r', s') is valid for m'.