Review Exercise Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

24.02.2012, WSH 24 A 407, 15:30h

Problem 4. Consider a parametrized hash function $h : \mathbb{N} \mapsto A$ given as

$$h(n) = \left\lfloor c\, f\left(\sqrt{2}\, n\right) \right\rfloor + d$$

with $f : \mathbb{R} \mapsto \mathbb{R}$ as $f(x) = x - \lfloor x \rfloor$, $\lfloor x \rfloor = \max\{k \in \mathbb{Z} \mid k \leq x\}$ and parameters $c, d \in \mathbb{N}$.

(a) Which properties should a cryptographic hash function have in general?

(b) What is the codomain A of the above hash function h?

(c) Find a collision for $(c, d) = (99, 1)$.

Alice has digitally signed two documents m_1 and m_2 by means of the ElGamal signature scheme. The public key of Alice is $(p, a, y) = (3733, 2, 1061)$ with p prime and a primitive element a modulo p. The documents have been hashed by the above hash function to $h(m_1) = 2138$ and $h(m_2) = 1531$, respectively. The corresponding signatures are

$$(r_1, s_1) = (557, 3153) \text{ and } (r_2, s_2) = (557, 1504).$$

(d) Which parameters (c, d) ensure that the above hash function is appropriate for this ElGamal signature scheme?

(e) What has Alice done wrong?

(f) Calculate the random secrets k_1 and k_2, respectively, and the private key x of Alice.

Problem 5. For a given prime p with $p = 4\,k - 1$, $k \in \mathbb{N}$ square roots modulo p shall be calculated. Let c be a quadratic residue modulo p.

(a) What is Euler's criterion?

(b) Show that $x_{1,2} \equiv \pm\, c^k \mod p$ solves $x^2 \equiv c \mod p$.

(c) Calculate the square roots of 7 modulo 47 and 5 modulo 79, respectively.

Consider the Rabin cryptosystem with parameters $p = 47$ and $q = 79$. Assume that the binary representation of the message ends with 101.

(d) Decrypt the ciphertext $c = 242$.
Hint: It holds $37 \cdot 47 - 22 \cdot 79 = 1$.

Problem 6. Consider the equation

$$E : Y^2 = X^3 + b.$$

(a) For which b does this equation describe an elliptic curve E over the field $\mathbb{F}_5$.

(b) For which b both points $(3, 1)$ and $(4, 4)$ are on $E(\mathbb{F}_5)$?

Now, take $b = 3$:

(c) Calculate all points on $E(\mathbb{F}_5)$. What is the trace t and the order of $E(\mathbb{F}_5)$?

(d) For each point on $E(\mathbb{F}_5)$, calculate its inverse.

(e) Show that point $(1, 2)$ generates $E(\mathbb{F}_5)$.

(f) Find all solutions of the equation $2P = \mathcal{O}$ in $E(\mathbb{F}_5)$.

(g) State the problem of the discrete logarithm on elliptic curves.