IV054 Coding, Cryptography and Cryptographic Protocols
2014 - Exercises VII.

1. Consider the DSA signature scheme. Let (p, q, r, x, y) be a key. Suppose the public parameters

$$p = 48731, \quad q = 443 \quad \text{and} \quad r = 5260.$$

The element r was computed as $r \equiv 7^{48730/443} \pmod{48731}$, where 7 is a primitive root modulo 48731. Alice chooses the secret signing key $x = 242$.

   (a) What is Alice's public verification key y?

   (b) Alice signs the digital document $D = 343$ using the ephemeral key $k = 427$. What is the signature? Perform all steps of her calculation and all steps of Bob's verification.

2. Consider the Ong-Schnorr-Shamir subliminal channel scheme with $k = 13$ and $n = 2109$. Compute in detail a signature for the message $w = 1759$ which contains secret $w' = 401$. Show that your signature is valid and that the decryption procedure works.

3. Consider the ElGamal signature scheme. Let (p, q, y) be a public key and let x be a secret key. Let i and j be integers with $\gcd(j, p-1) = 1$. Set

$$a \equiv q^i y^j \pmod{p}, \quad b \equiv -aj^{-1} \pmod{p-1}, \quad w \equiv -aij^{-1} \pmod{p-1}.$$

Prove that (a, b) is a valid ElGamal signature on the document w for the verification key y.

4. Consider the Lamport one-time signatures. Let $k = 5$.

   (a) For the function $f = 88^y \bmod 107$ and secret keys given in the table below compute the public keys and sign and verify the message 00101.

i	1	2	3	4	5
y_{i0}	91	2	44	99	82
y_{i1}	36	75	90	8	54

   (b) The designer of another Lamport scheme was lazy and forgot to limit the keys to one time use. You intercept two messages and their signatures:

$$(1, 0, 1, 1, 1, 58, 68, 97, 25, 78), \ (0, 0, 0, 1, 1, 98, 68, 62, 25, 78).$$

   Find all messages with their signatures you can now forge (without computing the logarithm).

   (c) Consider chosen signatures attack on this Lamport scheme where the keys are not one time use only. For general k, what is the minimal number of chosen signatures you need to obtain all the secret keys if all the public keys are unique.

5. Alice and Bob use the RSA signature scheme. Alice's public key is $(n, e) = (899, 17)$. Malicious Eve captured two signed messages which Alice sent: $(m_1, sign(m_1)) = (13, 644)$ and $(m_2, sign(m_2)) = (15, 213)$. Show that Eve is able to forge signatures of messages $m_3 = 195$ and $m_4 = 627$ without using brute force.

6. Consider the following signature scheme for a group of two users. Each of the users i has his own RSA signature scheme with public key (n_i, e_i) and secret key d_i, $i = 1, 2$. Their respective trapdoor one way permutation is $f_i(x) = x^{e_i} \pmod{n_i}$.

For b such that $2^b > \max(n_1, n_2)$ we define new trapdoor one way permutations g_i in the following way. For b-bit input x define integers q_i and r_i such that $x = q_i n_i + r_i$, $0 \leq r_i < n_i$ (we know r_i, q_i are unique). Then

$$g_i(x) = \begin{cases} q_i n_i + f_i(r_i) & \text{if } (q_i + 1)n_i \leq 2^b \\ x & \text{else} \end{cases}$$

More on next page >>>

Let h be public collision-resistant hash function that maps messages to b-bit strings.

Now the user i signs any message m as follows:

1. Computes the key $k = h(m)$
2. Choses random b-bit x_j, $j \neq i$.
3. Computes $y_j = g_j(x_j)$ using n_j, e_j.
4. Finds y_i such that $y_i \oplus y_j = k$.
5. Using d_i finds $x_i = g^{-1}(y_i)$.
6. Outputs the signature $((e_1, n_1), (e_2, n_2), x_1, x_2)$.

(a) Find the verification of the signature.

(b) Given a message and its signature, can you discover which user signed the message?