Cryptography and Architectures for Computer Security

Exam Code: 095947 (old 090959), A.Y. 2015–2016, Semester: 2

Prof. G. Pelosi

September 28th, 2016 – Exam Session

Name:.................................... Surname:..

Student ID:................................ Signature:...

Time: 2h:30'. Use of textbooks, notes, phones or Internet connected devices is not allowed. Prior to turn in your paper, write your name on any additional sheet and sign it.

Question 1 [2 pts]
Alice uses a block cipher `Enc` having 64-bit block size and 64-bit key size. She is worried that the key size is too small to prevent brute force attacks. Therefore, she decides to improve the encryption scheme employing 2 independent 64-bit keys: (k_0, k_1), and encrypting her messages as:

$$c = \mathtt{Enc}_{k_0}(m) \oplus k_1, \qquad m, c \in \{0,1\}^{64}$$

- Assume that the adversary gets access to a few plaintext/ciphertext pairs and is indeed able to perform a brute-force attack on the original encryption scheme `Enc` and recover the key with a *known plaintext attack*. Show that he can also break the "improved" scheme and recover the Alice's extended key.

Question 2 [3 pts]
Consider a file encrypted with a given mode of operation and the problem of decrypting only a single block in "the middle" of the available ciphertext (i.e., we are interested only in the n-th plaintext block, with $n>1$).

- Discuss how this can be done. Of course one can do it by decrypting the whole file, so the answer must describe how to solve the problem considering different mode of operations and point out the most efficient scenario.

Question 3 [3 pts]
We consider the possibility of using SHA-1 or SHA-2 for authentication as follows.
Bob authenticates a message m for Alice by computing $h(k||m||p)$ where $h(\cdots)$ is the hash function, k is a secret key shared between Alice and Bob, and p is padding.
Prove that this system has the (unwanted) property that the Adversary can authenticate certain messages not sent by Bob.

Question 4 [6 pts]
Consider multiplicative groups: $G_1 = \mathbb{Z}^*_{89}$, $G_2 = \mathbb{Z}^*_{97}$

(a) Show that 7 is a generator for both G_1 and G_2

(b) Solve the discrete logarithm problem $\log_7^{\mathtt{D}}(2)$ in G_1 and G_2

(c) Which discrete logarithm is harder, and why ?

Question 5 [5 pts]
Consider a schoolbook RSA encryption scheme with public and private key $k_{\mathtt{pub}} = \langle\, e, n\,\rangle$, $k_{\mathtt{priv}} = \langle\, p, q, \varphi(n), d\,\rangle$. Given a ciphertext $c \in (\mathbb{Z}_n, +, \cdot)$, a *chaining attack* aims to recover the corresponding plaintext $m \in (\mathbb{Z}_n, +, \cdot)$ without knowing the private key and exploiting the following computations:

$$c^e \bmod n, \quad c^{e^2} \bmod n, \quad \ldots, \quad c^{e^{k-1}}, \quad c^{e^k} \equiv c \bmod n$$

Thus the attacker aims to find the smallest integer k which allows him to observe a cycle.

(a) Assuming that the above mentioned k exists, show how to derive the plaintext.

(b) Explain why such a value $k \in \{1, \ldots, n-1\}$ always exists. Hint: Recall that RSA is an encryption algorithm and therefore bijective, i.e., $m_1^e \not\equiv_n m_2^e$, $\forall m_1, m_2 \in (\mathbb{Z}_n, +, \cdot)$

Question 6 [14 pts]

(a) Describe the Fermat primality test and the Miller-Rabin primality test.

(b) Apply the Pollard's ρ method to factor the RSA public modulus $n = p \cdot q = 1147$

(c) Let $e{=}49_{\mathtt{dec}}$ be the public exponent of an RSA public-key $k_{pub}{=}\langle e, n\rangle$. Knowing the factorization of the modulus n, compute the value of the corresponding RSA private-key $k_{priv}{=}(p, q, \varphi(n), d)$. Show every step of the computation.

(d) Decrypt the message $c{=}10_{\mathtt{dec}}{\in}\mathbb{Z}_n$ (provided without any padding scheme) through applying the CRT. Describe each step of the procedure.

(e) Describe the Optimized Asymmetric Encryption Padding (OAEP) scheme and the reasons to employ it in a non school-book implementation of the RSA cryptosystem.

(f) Assume to work into the Montgomery domain: $(\widetilde{\mathbb{Z}}_p, +, \times)$, $p{=}23$

- Given $A{=}5_{\mathtt{dec}}$, $B{=}7_{\mathtt{dec}}$, show the corresponding values in the Montgomery domain (i.e., $\widetilde{A}$, $\widetilde{B}$) justifying your answer.
- Compute the Montgomery multiplication $\widetilde{C}{=}\widetilde{A}{\times}\widetilde{B} \bmod p$, assuming a binary encoding of the operands.
- Explain the reasons to employ a Montgomery-based arithmetic for the efficient implementation of asymmetric cryptosystems.