Cryptography and Architectures for Computer Security

Exam Code: 095947 (old 090959), A.Y. 2014–2015, Semester: 2

Prof. G. Pelosi

July 20th, 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 [6 pts]
Alice and Bob wish to use a block cipher in either CBC or CTR mode of operation for exchanging encrypted data. An (active) adversary is able to intercept and change messages sent between Alice and Bob. Consider the following scenarios.

(a) In some messages sent by Bob, it is the case that the last block is a randomly generated secret key. For the two modes, establish whether the adversary can corrupt the transmitted messages, so that Alice receives a message that looks good after decryption, but contains the wrong key.

(b) In some messages sent by Bob, the adversary may know the first block M_1 and want to replace it by another block A_1 of his choice, leaving the rest of the message unchanged. Show that the adversary can achieve this if CTR mode of operation is employed. Do you think he can do it also with the CBC mode?

Question 2 [2 pts]
Consider a public-key based authentication procedure on an SSH server.

(a) Is it sensible to disable DSA keypairs to perform SSH user authentication, out of the concern that the SSH server may be running on a platform endowed with a relatively poor random number generator? Justify your answer coincisely but effectively.

(b) Is it possible to employ DSA as the only public key algorithm in an SSH authentication procedure (connection to established login)?

Question 3 [6 pts]

(a) Consider the cyclic group $(\mathbb{Z}_{25}^*, \cdot)$. Compute the cardinality of the group, the number of its generators and exhibit at least one generator for each of its subgroups

(b) Consider the group $(\mathbb{Z}_{45}^*, \cdot)$. Determine if the multiplicative inverses of x=4 and y=6 exist and compute their values.

(c) Consider the finite field $\mathbb{F}_{5^3}^*$. Determine if $f(x)=x^3-x-1 \in \mathbb{F}_5[x]$ is a primitive polynomial and show all its roots.

Question 4 [6 pts]
Consider the elliptic curve $\mathbb{E}(\mathbb{F}_5)$: $y^2{=}x^3{-}x$.

(a) Find the order of the group of points lying on $\mathbb{E}(\mathbb{F}_5)$, and the number of its generators.

(b) Compute $\mathtt{Q}{=}[9]\mathtt{P}$, with $\mathtt{P}{=}(2,1)$, showing each step of the computation.

(c) Explain the advantages of elliptic curve cryptosystems and describe the operations of the Elliptic Curve ElGamal encryption primitive.

Question 5 [12 pts]

(a) Consider the RSA modulus $n = p \cdot q = 133 = 7 \cdot 19$

- Apply the Miller-Rabin primality test to the factor p employing as bases $a = 2$, $b = 3$.
- Given the public exponent $e{=}7$, compute the value of the RSA private key, $k_{priv}{=}(p, q, \varphi(n), d)$ specifying every step of the computation.
- Apply a Square & Multiply strategy to sign the message $m{=}101 \bmod n$ employing a radix-4 encoding of the exponent, subsequently apply the CRT to sign again the same message (showing every step of the computation).

(b) Discuss working principles of the Montgomery Multiplication.

(c) Show how to implement the operations of the Diffie-Hellman protocol at each endpoint of the communication, employing the Montgomery multiplication primitive. Show a pseudo-code of the proposed implementation.

(d) Assume to work into the Montgomery domain: $(\widetilde{\mathbb{Z}}_n, +, \times)$, $n = 27$. Compute the multiplication between the following two values: $\widetilde{A} = 16_{\text{dec}}$ and $\widetilde{B} = 11_{\text{dec}}$, assuming a binary encoding of the operands and showing every step of the procedure.