Cryptography and Architectures for Computer Security

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

Prof. G. Pelosi

September 14th, 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**]
Consider a *chosen plaintext attack* scenario, where the adversary can submit a plaintext of her choice for symmetric-encryption. We adopt Kerckhoffs' principle and assume that the adversary knows the type of system used. Which choice of plaintext would he make if the crypto-system is:

(a) a shift cipher?

(b) a Vigenére cipher?

(c) a simple substitution cipher?

(d) a transposition cipher?

Question 2 [**2 pts**] Consider a a symmetric block cipher with a 128 bit block size, and a 128 bit key size, having a fully linear (non-singular) round function. Describe how it is possible to retrieve the secret key, under the assumption of a known plaintext attack stating also which are the requirements in terms of the quantity of plaintext and ciphertext to be known. The method should *not* resort to exhaustive key search.

Justify what is the change in the requirements for the attacker if the same block cipher is changed to employ a 256 bit key, while keeping all its other features the same.

Question 3 [**4 pts**] Consider the case of Linear Feedback Shift Registers (LFSRs), employed to generate a keystream which is combined via xor with the plaintext. State whether the following solutions can be broken knowing a portion of the keystream via simultaneous equations solutions, and the amount of keystream required to do so. If a precise value for the amount of bits cannot be stated state a reasonable estimate.

(a) A 128 bit sized LFSR, of which the inner state is unknown, but the primitive connection polynomial is known, is employed as keystream generator

(b) A 128 bit sized LFSR, of which it is only known that the connection polynomial is primitive, but its form is unknown is employed as keystream generator

(c) Two 128 bit LFSRs, of which it is only known that the connection polynomial is primitive, to a pair of keystream bits per clock cycle in the following fashion: the first LFSR has its output bit both output as the first element of the pair, and driving the clock of the second LFSR. The second LFSR simply outputs its output bit as the second of the pair.

(d) Two 128 bit LFSRs, of which it is only known that the connection polynomial is primitive, where the first LFSR output bit acts drives the clock for the second one, while the output of the second one is used as the keystream.

Question 4 [6 pts]

(a) Consider the cyclic group $(\mathbb{Z}^*_{27}, \cdot)$. 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 finite field $\mathbb{F}^*_{3^4}$. Find the number of irreducible and primitive polynomials. Determine if $f(x){=}x^4{+}x{+}2{\in}\mathbb{F}_3[x]$ is a primitive polynomial and show all its roots.

Question 5 [6 pts]

Consider the elliptic curve $\mathbb{E}(\mathbb{F}_{11})$: $y^2{=}x^3{+}x{+}6$.

(a) Find the order of the group of points lying on $\mathbb{E}(\mathbb{F}_{11})$, and the number of its generators.

(b) Consider an instance of the EC Diffie-Hellman protocol, assuming the base point $\mathtt{P}{=}(2,7){\in}\mathbb{E}(\mathbb{F}_{11})$ as generator of the group. What is the shared key when the secret ephemeral keys are 2 and 6, respectively?

(c) Discuss how to properly choose the public parameters of a discrete log based cryptosystem.

Question 6 [12 pts]

(a) Describe the Pollard's $p{-}1$ factoring method.

(b) Apply the Pollard's ρ method to factorize the RSA modulus $n = p \cdot q = 713$.
Assume $f(x) = x^2 + 1 \bmod n$ as "random-walking" function. Show every passage of the computation. (As a backup alternative, apply a "trivial division" strategy).

(c) Given the public exponent $e = 7 \in \mathbb{Z}^*_{\varphi(n)}$, show the value of the RSA private key, $k_{priv} = (p, q, \varphi(n), d)$ and specify every step of the computation.

(d) Sign the message $m{=}55 \in \mathbb{Z}_n$ (without employing any padding scheme) through applying the CRT: $s = m^d \bmod n$. Describe each step of the procedure.

(e) Assume to work into the Montgomery domain: $(\widetilde{\mathbb{Z}}_N, +, \times),\ N = 21$

- Show the definition of the Montgomery Multiplication and the smallest admissible value for the Montgomery Radix: R
- Show the high-level pseudo-code to implement the Montgomery Reduction procedure MRed(...), and prove the correctness of the algorithm.
- Compute a pair of integer values R', N' that satisfy the relation: $\gcd(R,N){=}R\,R'{-}N\,N'{=}1$, showing each step of the procedure
- Compute the Montgomery multiplication $\widetilde{C} = \widetilde{A} \times \widetilde{B} \bmod N$, where $\widetilde{A} = 17_{\text{dec}}$ and $\widetilde{B} = 6_{\text{dec}}$, assuming a binary encoding of the operands