Cryptography and Architectures for Computer Security

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

Prof. G. Pelosi

July 1st, 2015 – 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 [3 pts]
Consider a TLS ciphersuite as a tuple $(\mathcal{A}_{kex}, \mathcal{A}_{auth}, \mathcal{A}_{sym}, \mathcal{A}_{hash})$

(a) Which choice between *(Diffie-Hellman-2048, RSA-1024, AES-128-GCM, SHA-2-256)* and *(Diffie-Hellman-Ephemeral-512, RSA-2048, AES-128-GCM, SHA-2-256)* is the one providing the highest security margin?

(b) During the TLS key exchange, is it possible for an active attacker to alter the value of the session nonce, setting it to an arbitrary value decided by him?
Does this action get detected before the end of the TLS handshake?

(c) Is there any difference between picking *(Diffie-Hellman-Ephemeral-2048, RSA-2048, None, SHA-2-256)* and *(Diffie-Hellman-2048, RSA-2048, None, SHA-2-256)* as a TLS ciphersuite?

Question 2 [3 pts]
While reviewing an implementation of AES-128-CBC, you discover that it simply uses the last ciphertext block from the previously encrypted message as the `IV` value C_0 for encrypting the next message. The implementation's authors argue that as long as the `IV` of the very first message was chosen uniformly at random, all resulting subsequent ciphertext blocks will also be distributed uniformly at random, thus providing a secure solution[1].
Discuss the robustness of this CBC implementation with respect to a *Chosen Plaintext Attack*.

Question 3 [5 pts]
Consider a substitution-permutation block cipher with a 128-bit block and a 256-bit key, employing 32 identical 4×4 bit S-boxes for the substitution layer. The best (i.e., highest) linear bias for the S-Box is $\varepsilon = \frac{1}{8}$, while the highest differential probability is $\frac{1}{4}$. The permutation layer is built so that the 4 output bits of each S-Box are employed as inputs to four different boxes in the subsequent layer. The diffusion of the cipher is such that given a change in an S-box input at round i, 4 s-boxes

[1] The initial `IV` used by SSL 3.0 (TLS 1.0) was a (pseudo)random string generated and shared during the initial handshake phase, subsequent `IV`s were chosen following the deterministic pattern previously described.

will be involved at round $i+1$, 16 at round $i+2$ and all of them from round $i+3$ onwards. The cipher round acts on the state performing with the substitution layer, the permutation layer and the round key addition, in this order. A single key extra key addition is present before the first round takes place.

(a) Compute the value of a conservative estimate of the linear bias useful for retrieving the last round key for the described block cipher assuming it is 4 rounds long, and the amount of plaintext-ciphertext pairs available. Is it possibly broken by linear cryptanalysis?

(b) Compute the value of the differential probability useful for retrieving the last round key for the described block cipher assuming it is 4 rounds long, and the amount of plaintext-ciphertext pairs available. Is it possibly broken by differential cryptanalysis?

(c) Keeping the same round structure, and the same key length, is it possible to render the block linear and differential cryptanalysis immune? If yes, describe what should be tuned and to which extent.

Question 4 [6 pts]

(a) Name two advantages of using cyclic groups of *prime order* in cryptographic schemes that rely on the difficulty of the Discrete Logarithm Problem or the Diffie-Hellman Problem.

(b) Consider the cyclic group $(\mathbb{Z}^*_{169}, \cdot)$.

- How many generators are there?
- Determine one generator g of $\mathbb{Z}^*_{169}$ and exhibit at least one generator for largest (proper) subgroup of $\mathbb{Z}^*_{169}$.
- Denote as $G{=}\langle 40\rangle$ the largest prime subgroup of $(\mathbb{Z}^*_{169}, \cdot)$ and compute the discrete logarithm $x \equiv_{|G|} \log^{\mathtt{D}}_{40} 14$, applying the Baby-Step Giant-Step algorithm.

Question 5 [5 pts]
Consider an elliptic curve cryptosystem defined over the elliptic curve $\mathbb{E}(\mathbb{Z}_{11})$ with equation
$y^2 = x^3 + 1$ over $\mathbb{Z}_{11}$.

(a) What is the order of the additive group $(\mathbb{E}(\mathbb{Z}_{11}),\ +)$?

(b) What is the sum of the points (2, 3) and (5, 4)?

(c) Describe the encryption and decryption functions of the Elliptic Curve ElGamal cryptosystem.

Question 6 [8 pts]
Consider the RSA modulus $n{=}p{\cdot}q{=}899$

(a) Apply the Pollard's $\mathtt{P}{-}1$ factorization method to compute the two factors p and q (assuming $p{<}q$). Consider the factor p being B-power smooth, with $B{=}6$, while the factor q is not.[2]

(b) Sketch the pseudo-code (of one or more routines) needed for implementing the Pollard's $\mathtt{P}{-}1$ algorithm employed to answer to the previous question. Show the computational complexity of the proposed implementation.

[2] To solve the remaining parts of the exercise you can apply a trivial division algorithm as a back up factoring strategy

(c) Given the modulus factorization found as answer to (a), pick the value of an admissible secret exponent d among $d_1 = 3,\ d_2 = 35,\ d_3 = 121$, explaining the reasons of your choice.

(d) Sign the message $m{=}100_{\text{decimal}}{\in}\mathbb{Z}_n$ (provided without any padding scheme) through applying the CRT. Describe each step of the procedure.

Question 7 [4 pts]
Assume to work into the Montgomery domain: $(\mathbb{Z}_N, +, \times)$, $N = 15$.
Compute the Montgomery multiplication $C{=}A{\times}B \bmod N$, where $A{=}8_{\text{decimal}}$ and $B{=}11_{\text{decimal}}$ are binary encoded values in the Montgomery domain. Show every step of the procedure.