Cryptography and Architectures for Computer Security

Exam Code: 095947 (old 090959), A.Y. 2018–2019, Semester: 2

Prof. G. Pelosi

July 2nd, 2019

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

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

Time: 2h, 15min. Use of textbooks, notes, or Internet connected devices (including smartphones) is not allowed. The usage of simple calculators is allowed. Prior to turn in your paper, write your name on any additional sheet and sign it.

Question 1 [3 pts]
Consider an improved version of the Vigenère cipher, where instead of using multiple shift ciphers, multiple mono-alphabetic substitution ciphers are used. That is, the key consists of t random permutations of the alphabet, and the plaintext characters in positions i, $t+i$, $2t+i$, and so on, are encrypted using the ith permutation.
Show how to break this version of the cipher.

Question 2 [5 pts]
Consider a 128-bit block symmetric cipher, built with a Substitution-Permutation network approach. Two alternate designs are available, both employing a key addition via bitwise `xor`:

- Design A: 4×4 bit S-boxes, having a worst-case linear bias of $\frac{1}{8}$, and a worst case differential probability of $\frac{1}{4}$. Permutation layer built so that a single bit input to the permutation layer will affect four distinct S-Boxes on the next round.
- Design B: 8×8 bit S-Boxes, with worst-case linear bias of $\frac{1}{64}$ and worst-case differential probability of $\frac{1}{64}$. Permutation layer built so that a single bit input will affect two S-Boxes on the next round.

(a) What is the design that allows to build the shortest (in terms of number of rounds) block cipher, assuming a key length of 128 bits?

Question 3 [3 pts]
Consider the case of connections employing the TLS protocol.

(a) What is the advantage of exploiting a TLS based secure transport to build a point-to-point VPN with respect to an IPSec based alternative?

(b) Is it possible to detect TLS connection downgrades to an unwanted version assuming that only the client configuration can be chosen at will?

(c) Is it possible to do the same assuming that only the server configuration can be chosen at will?

Question 4 [6 pts]

(a) List the cardinality, number of subgroups and number of generators of the following multiplicative groups: $(\mathbb{Z}_{49}, \times)$ and $(\mathbb{F}^*_{7^2}, \cdot)$.

(b) $f(x) = x^2 + x + 3 \in \mathbb{F}_7[x]$ is a primitive polynomial for $\mathbb{F}_{7^2}$. Show the roots of $f(x)$ as elements of $\mathbb{F}_{7^2} \cong \{\theta_6\alpha^6 + \theta_5\alpha^5 + \ldots + \theta_1\alpha + \theta_0,\ \theta_i \in \mathbb{F}_7, 0 \le i \le 6\ f(\alpha) = 0\}$.

(c) The DSS-DSA standard recommends a public key with two primes p, q such that the pair (L, N), with $L = \log_2(p)$ and $N = \log_2(q)$, is in the following list: (1024,160), (2048,224), (2048,256), and (3072,256).
What is the purpose of p, q in the public key?
What is the reason for including q in the public key?

Question 5 [5 pts]

Consider the following relation: $13 \equiv 3^x \bmod 17$.

(a) Compute the discrete logarithm $x \equiv_{\varphi(17)} \log_3^{\mathrm{D}}(13)$ applying the Pohlig-Hellman method.

(b) Show the computational complexity of the Pohlig-Hellman algorithm. When is it appropriate to use this method?

Question 6 [12 pts]

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

(b) Apply the Pollard's ρ method[1] to factor the RSA public modulus $n = p \cdot q = 1357$

(c) Given the factorization of $n = p \cdot q$, note that $p = 2p_1 + 1$ and $q = 2q_1 + 1$, with p_1 and q_1 also prime numbers. Show the number of possible values for the RSA encryption exponent e as a function of p_1 and q_1 and compute its value. Subsequently, assuming $e = 5$, compute the corresponding RSA private key, justifying your answer.

(d) Assume that a smart-card contains an RSA co-processor with an hardcoded public modulus $n = 1541$, and a school-book implementation (no OAEP), leaving the choice of the public exponent to the user. Eve obtains two encryptions of the same message m with the following two public exponents: $e_{\mathrm{A}} = 5$, $e_{\mathrm{B}} = 7$.
Can she derive the plaintext message?
Motivate your answer and show every step of the computation.

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

- Exhibit the smallest admissible value for the Montgomery Radix, R, and the values R', p' that satisfy the relation: $\gcd(R, p) = R\,R' - p\,p' = 1$, justifying your answer;
- Compute the Montgomery multiplication $\widetilde{C} = \mathrm{MonPro}(\widetilde{A}, \widetilde{B}) = \widetilde{A} \cdot \widetilde{B} \cdot R^{-1} \bmod p$, where $\widetilde{A} = 16_{\mathrm{dec}}$ and $\widetilde{B} = 11_{\mathrm{dec}}$, assuming a binary encoding of the operands.

[1] as a back-up strategy you can apply a trivial division method