Cryptography and Architectures for Computer Security

Exam Code: 095947 (old 090959), A.Y. 2017–2018, Semester: 2

Prof. G. Pelosi

June 21st, 2018 – Exam Session

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

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

Time: 2h:30'. 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 [4 pts]

The CBC mode of operation requires an Initialization Vector, `IV`, as the initial ciphertext block to kick things off, and the `IV` must be **i)** Unique (i.e., must not be repeated for any message encrypted with a given key); and **ii)** Unpredictable (i.e., an attacker who observes any number of messages encrypted with a given key and their `IV`s should have no information to predict the next one with probability of success greater than 50% per bit – indistinguishable from random).

(a) explain why uniqueness property is necessary;

(b) explain why unpredictability property is necessary.

Question 2 [5 pts]

Consider the following 4 × 4 bit S-Box.

in	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
out	0001	0001	0111	0111	0110	0110	0000	0000	1100	1111	1110	1001	1000	1011	1101	1010

(a) Let $\langle b_3, b_2, b_1, b_0\rangle$ be the output bits of the S-Box above corresponding to the input $\langle a_3, a_2, a_1, a_0\rangle$. Compute the linear bias for the expression $a_2 \oplus a_0 = b_3 \oplus b_0$.

(b) Compute the probability of the differential $(\Delta a, \Delta b) = (0001, 0011)$ and of the differential $(\Delta a, \Delta b) = (0001, 0000)$. Which one is best employed by an attacker (without considering questions on the number of involved bits)?

Consider a block cipher with a 128-bit key and a *Substitution-Permutation Network* (SPN) design. The cipher has a 128-bit wide block. The *key addition layer* is performed via bitwise `xor`. The *substitution layer* of the cipher is constituted by 32 equal S-Boxes defined as shown above, and acting on 4 bits of the state each. The *linear permutation layer* is built in such a fashion that causes a single bit change in the output of an S-Box to propagate to four distinct S-Boxes in the next round.

Therefore, it can be assumed that a single bit change in the plaintext will involve one S-Box in the first round, 4 in the second, 16 in the third, and 32 from the fourth round onwards.

(c) Compute, employing the aforementioned assumptions and the linear bias obtained in (a), the minimum number of rounds for the cipher to be immune to linear cryptanalysis.

(d) Compute, employing the aforementioned assumptions and the highest probability obtained in (b), the minimum number of rounds for the cipher to be immune to differential cryptanalysis.

Question 3 [4 pts]
Consider the SSH protocol.

(a) It is often advised to avoid password-based authentication whenever possible, replacing it by per-user public key authentication. Such an advice comes from an advantage in case of a disclosure of the private key of the SSH server. Justify whether or not this is a correct advice.

(b) Consider a user, willing to generate a large number X of RSA user-authentication keypairs for SSH. In order to save time, the user generates only $\sqrt{X}$ distinct prime numbers and obtains the public moduli of the keypairs multiplying pairs of the said primes. Argue in favor or against the said procedure, and describe if the administrators of two distinct SSH servers where the user is authenticating with two separate keypairs may abuse of the said procedure.

Question 4 [9 pts]

(a) Consider the cyclic group $(\mathbb{Z}^*_{625}, \cdot)$. Compute the cardinality of the group, the number of its generators and the number of subgroups.

(b) Consider the finite field $\mathbb{F}_{5^4}$. Compute the cardinality of the multiplicative group. Find the number of irreducible and primitive polynomials. Determine if $f(x) = x^5 + 4x - 1 \in \mathbb{F}_5[x]$ is reducible or not.

(c) State the conditions to properly configure the public parameters of a Diffie-Hellman protocol justifying your answer. Which cyclic group between $(\mathbb{Z}^*_{625}, \cdot)$ and $(\mathbb{F}^*_{5^4}, \cdot)$ would be preferable?

Question 5 [14 pts]

(a) Apply the Pollard's ρ method to factorize the RSA modulus $n = p \cdot q = 667_{\text{dec}}$.
Assume $f(x) = x^2 + 1 \bmod n$ as the "random-walking" function. Show every step of the computation. (As a backup alternative, apply a "trivial division" strategy).

(b) Describe the Miller-Rabin and the Fermat primality tests, pointing out the reasons to prefer the former.

(c) Choose an admissible private exponent d between the values d=$31_{\texttt{dec}}$ and d=$77_{\texttt{dec}}$ and show the value of the corresponding RSA public and private keys k_{pub}=(e, n), k_{priv}=$(p, q, \varphi(n), d)$.

(d) Sign the message m=$500_{\texttt{dec}} \in \mathbb{Z}_n$ (without employing any padding scheme) through applying the CRT. Describe each step of the procedure.

(e) Consider a schoolbook RSA cryptosystem employing the Montgomery multiplication as building block. Write down the pseudo code of both the encryption and the CRT-based decryption transformations, pointing out their asymptotic computational complexities.

(f) Consider an RSA modulus $N = 3_{\text{dec}} \cdot 7_{\text{dec}} = 21_{\text{dec}}$. Compute the Montgomery multiplication between two operands $A = 18_{\text{dec}}$, $B = 17_{\text{dec}}$ that are already in the Montgomery domain $(\widetilde{\mathbb{Z}}_N, +, \times)$. Show every step of the computation, assuming a binary encoding of the operands and the smallest possible value for the Montgomery radix R.