Cryptography and Architectures for Computer Security

Exam Code: 095947 (old 090959), A.Y. 2016–2017, Semester: 2

Prof. G. Pelosi

July 5th, 2017 – 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 [9 pts]

(a) CBC-MAC works as the classic *Cipher Block Chaining* (CBC) mode of operation for encryption, with the only difference that the Initialization Vector (`IV`) must be a fixed value (usually zero), while the outputs consists of a single block – which is last block of the CBC-ciphertext.

Given a generic block cipher and a plaintext message m, explain why the composition of the following authenticated ciphertext does not provide message integrity.

$$C \leftarrow \texttt{CBC-Enc}_k(m||\texttt{MAC}_k(m))$$

where $\texttt{CBC-Enc}_k(\cdot)$ denotes the CBC-encryption mode of a block cipher encryption primitive $\texttt{Enc}_k(\cdot)$, while $\texttt{MAC}_k(m)$ denotes a MAC-CBC computation performed with the same key k.

(b) Compare the security guarantees of the following authenticated encryption procedures.

$$\begin{aligned} C &\leftarrow \texttt{ModeOfOperation-Enc}_{k_1}(m||\texttt{MAC}_{k_2}(m)), \text{ with } k_1 \neq k_2 \\ C &\leftarrow \texttt{ModeOfOperation-Enc}_{k_1}(m||\texttt{Signature}_{k_{\text{priv}}}(\texttt{hash}(m))) \end{aligned}$$

where `ModeOfOperation-Enc` is a primitive executing the encryption mode of a block cipher, `MAC` is a generic *Message Authentication Code*, and `Signature` is a generic public-key signature scheme.

(c) Public-key algorithms are usually used for encrypting short messages. But if we need to encrypt a longer message we can split it into blocks, use RSA for each block and then use a mode of operation to compute the ciphertext.
Which of the two modes between CBC and CTR would you recommend in such a situation? Why?

Question 2 [8 pts]
Consider the ring of polynomials $\mathbb{F}_2[x]$ in the unknown x.

(a) Is $\pi(x) = x^4 + x + 1$ irreducible? Is it primitive? Prove explicitly your answer.

(b) Representing $\mathbb{F}_{2^4}$ as $\mathbb{F}_2[x]/\pi(x)$, you are planning to design a 4×4 bits S-BOX, which can be described in compact form considering the four input bits $\langle a_3, a_2, a_1, a_0 \rangle$ as the coefficients of an element of $\mathbb{F}_{2^4}$, i.e., $a(x) = a_3x^3 + a_2x^2 + a_1x^1 + a_0$. Justify which one between the following three choices is the best one for the S-BOX function, taking into account their resistance to linear and differential cryptanalyses:

- SBOX-1$(a) = a^4$
- SBOX-2$(a) = a^3 + a + 1$
- SBOX-3$(a) = a^{16}$

(c) Complete SBOX-4(a), writing down its complete representation in the lookup table below.

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								

To this end,you may find useful the following equalities:
$x^4 = x + 1$
$x^5 = x^2 + x$
$x^6 = x^3 + x^2$

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 $a_2 \oplus a_0 = b_3 \oplus b_0$.
Compute the probability of the differential $(\Delta a, \Delta b) = (0001, 0011)$ and of the differential $(\Delta a, \Delta b) = (0001, 0000)$.

Question 3 [4 pts]
Consider the cyclic group $(G, \cdot)$=$\langle g \rangle$=$(\mathbb{Z}_p^*, \cdot)$, with p a large prime, and g a generator, and analyze the following digital signature scheme. The private key is defined as k_{priv}=$s \in \{0, 1, \ldots, p-1\}$, while the public key is defined as k_{pub}=$g^s \in G$.

To sign a message $m \in \{0,1\}^*$, one first computes the digest h=$H(m) \in (\mathbb{Z}_{p-1}^*, \cdot)$ for some, properly defined, hash function. Obs.: $\mathbb{Z}_{p-1}^* = \{a \mid 1 \leq a \leq p-1 \wedge \texttt{gcd}(a, p-1)=1\}$.

The signature $\sigma \in G$ is computed as $\sigma = g^{s \cdot h^{-1}}$, while the signature verification procedure executes the following check: $\sigma^h \overset{?}{=} k_{\text{pub}}$.

(a) Will correct signatures be accepted?

(b) Is it unfeasible to sign an arbitrary message without knowing the private key?

Question 4 [14 pts]

(a) Apply the Pollard's ρ method to factorize the RSA modulus $n = p \cdot q = 899$.
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 two primality tests.

(c) Choose an admissible public exponent e between the values $e{=}21_{\mathtt{dec}}$ and $e{=}143_{\mathtt{dec}}$ and compute the value of the corresponding RSA private key $k_{\text{priv}}{=}(p, q, \varphi(n), d)$. Show every step of the computation.

(d) Sign the message $m{=}898_{\mathtt{dec}}{\in}\mathbb{Z}_n$ (without employing any padding scheme) through applying the CRT. Describe each step of the procedure.

(e) Consider a double RSA encryption using two public keys $k_{\text{pub}-1}$, $k_{\text{pub}-2}$ with the same modulus N and two distinct public exponents (namely, e_1 and e_2, $\gcd(e_1, e_2) \neq 1$). Denote as d_1 and d_2 the private exponents corresponding to the the first and the second public key, respectively. A message m is encrypted using the RSA encryption transformation with the first public exponent e_1, and the result is encrypted again using e_2.
Does this scheme increase the security of the RSA cryptoscheme? Please, explain the reasons underlying your answer.

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

- Compute the following Montgomery multiplication assuming a binary encoding of the operands.
  $\widetilde{C}{\leftarrow}\widetilde{A}{\times}\widetilde{B} \bmod N$, with $\widetilde{A}{=}16_{\text{dec}}$ and $\widetilde{B}{=}15_{\text{dec}}$