Cryptography and Architectures for Computer Security

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

Prof. G. Pelosi

February 23rd, 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 [3 pts]
Why, in general, do practical public key cipher systems need larger block and key sizes than symmetric cipher systems?

Solution:
see lectures...

Question 2 [3 pts]
A *One Time Pad* encryptor machine trying to cope with broken random number generators does not encrypt the message with a keystream equal to either a sequence of 0s or a sequence of 1s. Is this enhancement affecting positively the security of the system? Motivate your answer.

Solution:
see lectures...

Question 3 [4 pts]
The post office of Lytia employs a digital authentication system to check the authenticity of package delivery electronic receipts.

(a) A first system relies on the digest of a custom keyed SHA-2-256 hash function, obtained from the original SHA-2-256 design permuting the order of the 8 32-bit initialization constants with a secret permutation.
Argue for or against the possibility of forging these keyed digests.

(b) A second system relies on the digest of a standard SHA-2-512 hash function fed with the concatenation of a 256-bit secret key (shared among the post offices) and a message.
Argue for or against the possibility of forging these keyed digests. (Assume that the disclosure of the secret key is not an option)

Solution:
see lectures...

Question 4 [6 pts]
Consider an elliptic curve cryptosystem defined over the elliptic curve $\mathbb{E}(\mathbb{F}_{13})$ with equation $y^2 = x^3 + 2$ over $\mathbb{F}_{13}$.

(a) What is the order of the additive group $(\mathbb{E}(\mathbb{F}_{13}), +)$?

(b) What is the sum of the points $(1, 4)$ and $(2, 6)$?

(c) To choose a safe curve for an ECC implementation, what are the desirable properties of the order of the curve?

Solution:

(a) $|\mathbb{E}(\mathbb{F}_{13})| = 19$

x, y	0	1	2	3	4	5	6	7	8	9	10	11	12
$x^3 + 2 \bmod 13$:	2	3	10	3	1	10	10	7	7	3	1	7	1
$y^2 \bmod 13$	0	1	4	9	3	12	10	10	12	3	9	4	1

Punti sulla curva	
(1, 4)	(1, 9)
(2, 6)	(2, 7)
(3, 4)	(3, 9)
(4, 1)	(4, 12)
(5, 6)	(5, 7)
(6, 6)	(6, 7)
(9, 4)	(9, 9)
(10, 1)	(10, 12)
(12, 1)	(12, 12)
	$\mathcal{O}$

(b) $(1, 4) + (2, 6) = (1, 9)$

(c) see lectures...

Question 5 [6 pts]
For the prime $p = 503$, the value $g = 5$ generates the full group $(\mathbb{Z}_p^*, \cdot)$.

(a) Encrypt the message $m = 42$ using the (school-book) ElGamal cryptosystem, employing $l{=}9{\in}\mathbb{Z}_{p-1}^*$ as the value returned by a random number generator.
Let us denote as $s \in \mathbb{Z}_{p-1}$ the secret key value, and consider the public key to be equal to $k_{\mathsf{pub}} = \langle n, g, g^s \rangle = \langle 502, 5, 383 \rangle$.

(b) Explain how an attacker who intercepts an ElGamal ciphertext and somehow knows the random value l, is able to decrypt, without knowledge of the private key.

(c) Assume that the system random number generator is stuck at a fixed randomly generated value l, and assume that an adversary is able to obtain a valid plaintext-ciphertext pair m_1, c_1. Show that in such a scenario, the attacker is able to decrypt any ciphertext she comes by.

Solution:
(sketch)
ciphertext: $c = \langle \gamma, \delta \rangle = \langle 479, 216 \rangle$;
$\gamma = g^l \bmod p = 479$;
$\delta = m \cdot (g^s)^l \bmod p = 216$
see lectures...

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 $n = p \cdot q = 851$

(c) Compute the value of the RSA private key, assuming a public exponent $e_A = 5$.

(d) Assume that a smart-card contains an RSA co-processor with an hardcoded public modulus $n = 851$, 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: $e_A = 5$, $e_B = 7$.
Can she derive the plaintext message?
Motivate your answer and show every step of the computation.

(e) Assume to use the Montgomery arithmetics for a software implementation of an RSA cryptosystem. Show the pseudo-code of the encryption and decryption (with CRT) primitives, defining all the appropriate sub-routines.

What are theoretical speedups of these implementations with respect to the school-book implementations of the encryption and decryption functions?

Solution:
(sketch)
$n = 851$;
$p = 23$, $q = 37$;
$\varphi(n) = 792 = 2^3 \cdot 3^2 \cdot 11$;
$\varphi(\varphi(n)) = 4 \cdot 6 \cdot 10 = 240$;
$d = e_A^{\varphi(\varphi(n))-1} \bmod \varphi(n) \equiv_{792} 5^{239} \equiv_{792} \ldots \equiv_{792} 317$;

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