Cryptography and Architectures for Computer Security

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

Prof. G. Pelosi

July 20th, 2016 – 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 [6 pts]
Alice and Bob wish to use a block cipher in either CBC or CTR mode of operation for exchanging encrypted data. An (active) adversary is able to intercept and change messages sent between Alice and Bob. Consider the following scenarios.

(a) In some messages sent by Bob, it is the case that the last block is a randomly generated secret key. For the two modes, establish whether the adversary can corrupt the transmitted messages, so that Alice receives a message that looks good after decryption, but contains the wrong key.

(b) In some messages sent by Bob, the adversary may know the first block M_1 and want to replace it by another block A_1 of his choice, leaving the rest of the message unchanged. Show that the adversary can achieve this if CTR mode of operation is employed. Do you think he can do it also with the CBC mode?

Solution:

(a) For both modes it is the case that the adversary can replace the last ciphertext block with any other block. When Alice decrypts the message all previous blocks will be unchanged and the message looks good; the last block will be corrupt, but since it is random, there is no way for Alice to discover this.

(b) The adversary can achieve this if CTR mode is employed. The encryption of the first block is $C_1{=}M_1{\oplus}Enc_K(IV||\texttt{ctr})$, thus he can derive $Enc_K(IV||\texttt{ctr}){=}C_1{\oplus}M_1$. In order to replace the first ciphertext block C_1 with $C_1'{=}A_1{\oplus}(\,Enc_K(IV||\texttt{ctr})\,)$, the adversary can compute $C_1'{=}A_1{\oplus}(\,C_1 \oplus M_1\,)$. Every other block remains unaffected by the modification made on the first one.

When the CBC mode is employed:
$C_0{=}IV$ (sent in clear),
$C_1{=}Enc_K(C_0{\oplus}M_1)$,
$C_2{=}Enc_K(C_1{\oplus}M_2)$,
...,

and
M_1=$Dec_K(C_1)\oplus C_0$,
M_2=$Dec_K(C_2)\oplus C_1$,
...,
In order to replace M_1 with A_1 without affecting M_2, the adversary can try to find another value for C_0 such that:
$C_0 \oplus M_1 = C_0' \oplus A_1$
thus, he can replace the IV value with C_0'=$C_0\oplus M_1\oplus A_1$ obtaining his goal, without changing C_1 or any other ciphertext block.

Question 2 [2 pts]
Consider a public-key based authentication procedure on an SSH server.

(a) Is it sensible to disable DSA keypairs to perform SSH user authentication, out of the concern that the SSH server may be running on a platform endowed with a relatively poor random number generator? Justify your answer coincisely but effectively.

(b) Is it possible to employ DSA as the only public key algorithm in an SSH authentication procedure (connection to established login)?

Solution:

(a) No. In user authentication, it is the user platform which both generates the required keypair, and performs the signatures, so there is no concern in a possible catastrophic failure of DSA due to a repeated random drawn in the signing process, or a keypair being generated with poor entropy.

(b) No. DSA is only able to provide authentication by means of performing/verifying cryptographic signatures: the SSH login requires a key exchange algorithm to choose a key to perform the user authentication phase.

Question 3 [6 pts]

(a) Consider the cyclic group $(\mathbb{Z}_{25}^*, \cdot)$. Compute the cardinality of the group, the number of its generators and exhibit at least one generator for each of its subgroups

(b) Consider the group $(\mathbb{Z}_{45}^*, \cdot)$. Determine if the multiplicative inverses of x=4 and y=6 exist and compute their values.

(c) Consider the finite field $\mathbb{F}_{5^3}^*$. Determine if $f(x)$=$x^3-x-1\in\mathbb{F}_5[x]$ is a primitive polynomial and show all its roots.

Solution:

(a) n=$|(\mathbb{Z}_{25}^*, \cdot)|$=$\varphi(25)$=20.
No. of generators=$\varphi(n)$=$\varphi(2^2 \cdot 5)$=8.
g=2 is a generator: the proper divisors of n are 2, 4, 5, 10, and

$$\begin{cases} g^{\frac{n}{2}} \equiv_{25} g^{10} \equiv_{25} 24 \not\equiv 1 \\ g^{\frac{n}{4}} \equiv_{25} g^{5} \equiv_{25} 7 \not\equiv 1 \\ g^{\frac{n}{5}} \equiv_{25} g^{4} \equiv_{25} 16 \not\equiv 1 \\ g^{\frac{n}{10}} \equiv_{25} g^{2} \equiv_{25} 4 \not\equiv 1 \end{cases}$$

$H_1 = \langle 1 \rangle$, $|H_1| = 1$
$H_2 = \langle 24 \rangle$, $|H_2| = 2$
$H_4 = \langle g^{\frac{n}{4}} \equiv 7 \rangle$, $|H_4| = 4$
$H_5 = \langle g^{\frac{n}{5}} \equiv 16 \rangle$, $|H_5| = 5$
$H_{10} = \langle g^{\frac{n}{10}} \equiv 4 \rangle$, $|H_{10}| = 10$
$H_{20} = (\mathbb{Z}_{25}^*, \cdot) = \langle g \equiv 2 \rangle$, $|H_{20}| = 20$

(b) $x \in (\mathbb{Z}_{45}^*, \cdot)$, $y \notin (\mathbb{Z}_{45}^*, \cdot)$
$gcd(45, x) = 1 \Leftrightarrow 45 \cdot \xi + x \cdot \eta = 1$
applying the Extended Euclidean Algorithm ...
$\xi = 1$, $\eta = -11 \Rightarrow x^{-1} = (-11 \bmod 45) \equiv_{45} 34$

(c) $n = |(\mathbb{F}_{5^3}^*, \cdot)| = 124 = 2^2 \cdot 31$.
Making the hypothesis that $f(x) \in \mathbb{F}_5[x]$ is a primitive polynomial employed to build the representation of the field and denoting as $\alpha \in \mathbb{F}_{5^3}^* \setminus \mathbb{F}_5$ one of its roots (i.e.: $\alpha^3 = \alpha + 1$), it should be true that:

$$\begin{cases} \alpha^2 \not\equiv 1 \\ \alpha^4 \not\equiv 1 \\ \alpha^{31} \not\equiv 1 \\ \alpha^{62} \not\equiv 1 \end{cases}$$

$\alpha^4 \equiv \alpha^2 + \alpha$.
$\alpha^{31} \equiv ((\alpha^3)^5)^2 \cdot \alpha \equiv ((\alpha+1)^5)^2 \cdot \alpha \equiv (\alpha^5+1)^2 \cdot \alpha \equiv (\alpha^2+\alpha+2)^2 \cdot \alpha \equiv (\alpha^2+2\alpha+1) \cdot \alpha$
$\equiv 2\alpha^2 + 2\alpha + 1$.
$\alpha^{62} \equiv (2\alpha^2 + 2\alpha + 1)^2 \equiv \ldots \equiv 2\alpha^2 + \alpha - 1$.

$f(x) \in \mathbb{F}_5[x]$ is primitive.
Its roots are:
α,
$\alpha^5 \equiv \alpha^2 + \alpha + 1$,
$\alpha^{25} \equiv (\alpha^2+\alpha+1)^5 \equiv \alpha^{10} + \alpha^5 + 1 \equiv (\alpha^2 + \alpha + 1)(\alpha^2 + \alpha + 2) + 1 \equiv \ldots \alpha$

Question 4 [6 pts]
Consider the elliptic curve $\mathbb{E}(\mathbb{F}_5)$: $y^2 = x^3 - x$.

(a) Find the order of the group of points lying on $\mathbb{E}(\mathbb{F}_5)$, and the number of its generators.

(b) Compute `Q`$=[9]$`P`, with `P`$=(2, 1)$, showing each step of the computation.

(c) Explain the advantages of elliptic curve cryptosystems and describe the operations of the Elliptic Curve ElGamal encryption primitive.

Solution:

(a) $(0, 0)$ $(1, 0)$ $(4, 0)$ $(2, 1)$ $(2, 4)$ $(3, 2)$ $(3, 3)$ $\mathcal{O}$.
No. of group points: $n = 8$.
No. of generators = No. of positive integers that are less than n and coprime with n $= \varphi(n) = 4$.

(b) `Q`$=[9]$`P`$=[9 \bmod n]$`P`$=$`P`$=(2, 1)$.

(c) see lectures...

Question 5 [12 pts]

(a) Consider the RSA modulus $n = p \cdot q = 133 = 7 \cdot 19$

- Apply the Miller-Rabin primality test to the factor p employing as bases $a = 2$, $b = 3$.
- Given the public exponent e=7, compute the value of the RSA private key, k_{priv}=$(p, q, \varphi(n), d)$ specifying every step of the computation.
- Apply a Square & Multiply strategy to sign the message m=101 mod n employing a radix-4 encoding of the exponent, subsequently apply the CRT to sign again the same message (showing every step of the computation).

(b) Discuss working principles of the Montgomery Multiplication.

(c) Show how to implement the operations of the Diffie-Hellman protocol at each endpoint of the communication, employing the Montgomery multiplication primitive. Show a pseudo-code of the proposed implementation.

(d) Assume to work into the Montgomery domain: $(\widetilde{\mathbb{Z}}_n, +, \times)$, $n = 27$. Compute the multiplication between the following two values: $\widetilde{A} = 16_{\text{dec}}$ and $\widetilde{B} = 11_{\text{dec}}$, assuming a binary encoding of the operands and showing every step of the procedure.

Solution:

(a) for the Miller-Rabin test see lectures...
k_{priv}=$(p, q, \varphi(n), d)$=$(7, 19, 108, d \equiv_{108} 7^{\varphi(108)-1} \equiv_{108} 7^{35} \equiv_{108} 31)$
$s = Sign_{k_{priv}}(m) \equiv_{133} 101^{31_{\text{dec}}} \equiv_{133} 101^{133_4} \equiv_{133} (101^4 \cdot 101^3)^4 \cdot 101^3 \equiv_{133} (4 \cdot 83)^4 \cdot 101^3 \equiv_{133} 25 \cdot 101^3 \equiv_{133} 80$
for the application of CRT, see lectures.

(b) see lectures...

(c) see lectures...

(d)

$\lceil \log_2 n \rceil = 5,\ R = 2^5 = 32,$
$\gcd(R, N) = R \cdot R' - n \cdot n' = 1 \Leftrightarrow \gcd(32, 27) = 32(11) - 27(13) = 1,$
$R' \stackrel{\text{def}}{=} R^{-1} \bmod n = 11 \bmod 27 = 11,$
$n' \stackrel{\text{def}}{=} n^{-1} \bmod R = 13 \bmod 32 = 13;\ n'_0 = 1$

$\widetilde{B} = \langle B_4 B_3 B_2 B_1 B_0 \rangle = \langle 01011 \rangle_2$
$\widetilde{A} = \langle A_4 A_3 A_2 A_1 A_0 \rangle = \langle 10000 \rangle_2$

00000	+
00000	$A_0 B = 0 \cdot \langle 00000 \rangle_2$
00000	+
00000	$t\, n = (n'_0\, x_0)\, n = 0$
00000	perform a right-shift of 1 bit
⋮	+
⋮	$A_i B = 0 \cdot \langle 01011 \rangle_2$, $\mathbf{i = 1, 2, 3}$
⋮	+
⋮	$t\, n = (n'_0\, x_0)\, n = 0$, $\mathbf{i = 1, 2, 3}$
00000	perform a right-shift of 1 bit
00000	+
01011	$A_4 B = 1 \cdot \langle 01011 \rangle_2$
01011	+
11011	$t\, n = (n'_0\, x_0)\, n = 11011$
100110	perform a right-shift of 1 bit
10011	

$C = \langle 10011 \rangle_2 = 19 < n \Rightarrow \widetilde{C} = 16 \times 11 = 19 \in (\widetilde{\mathbb{Z}}_n, +, \times)$

Validation:

$\widetilde{C}$=$16 \times 11 \stackrel{\text{def}}{=} 16 \cdot 11 \cdot R^{-1} \bmod n$=$16 \cdot 11 \cdot 11 \bmod 27$=$19 \bmod 27$