Cryptography and Architectures for Computer Security

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

Prof. G. Pelosi

September 9th, 2015 – 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**]

(a) What are the choices of RSA and DSA key lengths to provide a sufficient security to be employed with a 128-bit symmetric cipher? What are the ones for a 256-bit symmetric cipher?

(b) Discuss if and when re-encrypting a message with the same block cipher employing different keys improves the security of system.

(c) Discuss if re-encrypting a message with an RSA cryptosystem employing different public exponents and the same public modulus improves the security of system.

Solution:
RSA – public modulus size: 3072-bit ($\equiv$ AES-128 security) 15360 ($\equiv$ AES-256 security)
DSA – group and pub. key sizes: 3072-bit; private key size: 256-bit ($\equiv$ AES-128 security)
DSA – group and pub. key sizes: 15360-bit; private key size: 512-bit ($\equiv$ AES-256 security),
See lectures...

Question 2 [**2 pts**]

(a) To define a cryptographic hash function, assume the input message m to be divided into l blocks of length L bits: $m = \langle m_1, m_2, \cdots, m_l \rangle$. Let $h(x) = m_1 \oplus m_2 \oplus \cdots \oplus m_l$.
Is $h(\cdot)$ a good cryptographic hash function?

(b) Describe the Merkle–Damgård design of hash functions and show how to realize a proper "keyed" hash function with it.

Solution:
See lectures...

Question 3 [4 pts]

(a) Are there any differences in signing an integer value a representing an amount of money with RSA and signing $\texttt{SHA-2}(a)$?

(b) Consider the case where a user decides to employ his RSA secret decryption exponent d also as his static Diffie-Hellman secret exponent, to lower the stress imposed on the system random number generator.

- Is it possible to violate the communication confidentiality whenever the DH-agreed key is used?
- Is it possible to violate message authentication provided via RSA signatures for some messages? if yes, how?

Solution:
See lectures...

Question 4 [6 pts]
Consider the multiplicative cyclic group $G=(\mathbb{Z}^*_{49}, \cdot)$:

(a) Show the number of generators and the values of at least two of them, denoting them g and h, respectively. Discuss the existence of the following discrete logs and compute them, if possible.

$$x_0=\log^{\mathsf{D}}_g 35$$
$$x_1=\log^{\mathsf{D}}_g 25$$
$$x_2=\log^{\mathsf{D}}_h 25$$
$$x_3=\log^{\mathsf{D}}_h (25 \cdot g)$$

(b) Show the value of the generators of the two largest (proper) subgroups.

(c) What are the criteria for selecting the parameters of a Diffie-Hellman key exchange protocol based on the algebra of cyclic groups?

Solution:

(a) $n = |G| = \varphi(49) = 42 = 2 \cdot 3 \cdot 7$
num. of generators $= \varphi(42) = 12$.
$g = 3, h = g^5 \equiv_{49} 3^5 \equiv_{49} 47$
The argument of the first dlog does not belong to G, as $gcd(35, n) \neq 1$, therefore x_0 does not exist.
$x_1=\log^{\mathsf{D}}_g 25 \equiv_{42} \log^{\mathsf{D}}_3 25 \equiv_{42} \cdots$ (Baby-step/Giant-step)$\cdots \equiv_{42} 16$

$x_2=\log^{\mathsf{D}}_h 25 \equiv_{42} x_1 \cdot (\log^{\mathsf{D}}_g h)^{-1} \equiv_{42} x_1 \cdot 5^{-1} \equiv_{42} 16 \cdot 17 \equiv_{42} 20$

$x_3=\log^{\mathsf{D}}_h (25 \cdot g) \equiv_{42} x_1 + \log^{\mathsf{D}}_h g \equiv_{42} x_1 + (\log^{\mathsf{D}}_g h)^{-1} \equiv_{42} 16 + 17 \equiv_{42} 33$

(b) g_1=9, g_2=27

(c) ...

Question 5 [6 pts]
Alice employs the Elliptic Curve Digital Signature standard (EC-DSA) protocol to sign her messages. Denoting as $\mathcal{O}$ the point at infinity, assume the following public parameters of the scheme.

$$\mathbb{E}(\mathbb{F}_{31}) : \{x, y \in \mathbb{F}_{31} \text{ s.t. } y^2 = x^3 + 9x + 1\} \cup \{\mathcal{O}\}$$

n=$|\mathbb{E}(\mathbb{F}_{31})|$=35 (order of the curve), P=$(7, 2)$ (base point).

(a) Compute the order of P, and Q=$-P$ justifying every passage.

(b) Compute the signature of the message $m_1 \in \{0, 1\}^*$, that is: $(k_1,\ z_1)$=$\text{Sign}^{\text{EC-DSA}}_{k_{priv}}(m_1)$, assuming digest e_1=SHA-1$(m_1) \equiv_{35} 12$, r=$8 \in \mathbb{Z}^*_n$ as random nonce extracted by the signature procedure, and s=31 as Alice's private key.

(c) Alice sends another signed message as a pair $\langle m_2, (k_2, z_2)\rangle$.
The message $m_2 \in \{0, 1\}^*$ has digest e_2=SHA-1(m_2) mod $n \equiv_{35} 18$, and the signature is $(k_2,\ z_2)$=$\text{Sign}^{\text{EC-DSA}}_{k_{priv}}(m_2)$=$(28, 32)$.
An adversary is able to collect the data transmitted with both messages and derive the Alice's secret key.
Explain the mistake made by Alice and show the computation made by the adversary to derive the value of the secret key s.

Hint: *EC-DSA Signature Algorithm*: $k_{priv} \leftarrow (s)$, $s \in \mathbb{Z}_n$ and $k_{pub} \leftarrow (n, \text{P}, [s]\text{P})$

```
1. $r \overset{\text{Random}}{\leftarrow} \{1, \ldots, n-1\},\ \gcd(r, n) = 1$
2. $[r]\text{P} = (x_1,\ y_1),\ k \leftarrow x_1 \bmod n.$ if $k = 0$ then go to step 1.
3. $e \leftarrow \text{SHA-1}(m)$
4. $z \leftarrow r^{-1}(e + s \cdot k) \bmod n.$ if $z = 0$ then go to step 1.
5. $\text{Sign}^{\text{EC-DSA}}_{k_{priv}}(m) = (k,\ z)$
```

Solution:

(a) Being n=35=$5 \cdot 7$, $P = (7, 2)$ is a generator iif $[5]P$ and $[7]P$ are different from $\mathcal{O}$.

$[2]P = [2](7, 2)$
$\lambda \equiv_{31} \frac{3 \cdot 7^2 + 9}{2 \cdot 2} \equiv_{31} \frac{156}{4} \equiv_{31} 39 \equiv_{31} 8$
$x_{[2]P} = 8^2 - 2 \cdot 7 \equiv_{31} 19$
$y_{[2]P} = -2 + 8 \cdot (7 - 19) \equiv_{31} 26$
$[2]P = (19, 26)$

$[3]P = [2]P + P = (19, 26) + (7, 2)$
$\lambda \equiv_{31} \frac{26-2}{19-7} \equiv_{31} \frac{24}{12} \equiv_{31} 2$
$x_{[3]P} = 2^2 - 19 - 7 \equiv_{31} 9$
$y_{[3]P} = -2 + 2 \cdot (7 - 9) \equiv_{31} 25$
$[3]P = (9, 25)$

$[5]P = [3]P + [2]P = (9, 25) + (19, 26) = \ldots = (12, 15)$

$[7]P = [5]P + [2]P = (12, 15) + (19, 26) = \ldots = (5, 27)$

$Q{=}{-}P{=}[n{-}1]P{=}(7, -2) = (7, 29)$ is also a generator.
Indeed, $|Q|{=}|{-}P|{=}|[n{-}1]P|{=}\ \frac{|P|}{\gcd(|P|,|[n-1]P|)}{=}\frac{n}{\gcd(n,n-1)}{=}n$

(b) $r = 8 \in \mathbb{Z}_n^*$ (random)
$R_1 = [r]P = [8](7, 2) = [7]P + P = (28, 28)$, $k_1 = x_R \bmod n = 28$
$z_1 = r^{-1}(e_1 + s \cdot k_1) \bmod n \equiv_{35} 22(12 + 31 \cdot 28) \equiv_{35} 5$
$(k_1, z_1) = (28, 5)$

(c) note that $k_1{=}k_2{=}28$, the secret key s can be derived solving two simultaneous equations in the unknowns r, s.

Question 6 [9 pts]

(a) Apply the Pollard's ρ method[1] to factor the RSA public modulus $n = p \cdot q = 1517$

(b) Given the private exponent $d{=}997 \bmod \varphi(n)$, compute the corresponding RSA public exponent employing the extended Euclidean algorithm

(c) Apply the CRT algorithm to sign the plaintext message $m{=}42{\in}\mathbb{Z}_n$

(d) Assume to work into the Montgomery domain: $(Z_N, +, \times)$. $N{=}27$. Compute the Montgomery multiplication $C{=}A{\times}B \bmod N$, where $A{=}\ 19_{\text{decimal}}{=}103_4$ and $B{=}\ 23_{\text{decimal}}{=}113_4$ are Radix-4 encoded values in the Montgomery domain. Show every step of the procedure, performing all the computations in Radix-4.

Solution:

(a) $\ldots p = 37, q = 41$

(b) $\varphi(n) = 36 \cdot 40 = 1440 \ldots$ (Euclid's method) $\ldots e \equiv_{1440} 13$

(c) $s \equiv_n c^d \equiv_{1517} 42^{997 \bmod 1440} = \ldots = 944$

(d) $b = 4$, $\lceil \log_b N \rceil = \lceil \log_4 27 \rceil = 3$, $R = b^3 = 64_{decimal}$
$gcd(R, N) = RR' - NN' = 1 \Leftrightarrow gcd(64_{dec}, 27_{dec}) = 64_{dec}(-8)_{dec} - 27_{dec}(-19)_{dec}$
$\Rightarrow R' \overset{\text{def}}{=} R^{-1} \bmod N = -8_{\text{dec}} \bmod 27 \equiv_{27} 19_{\text{dec}}$
$\Rightarrow N' \overset{\text{def}}{=} N^{-1} \bmod R = -19_{\text{dec}} \bmod 64 = 45_{\text{dec}} \bmod 64 \equiv_{64} 231_4 \Rightarrow N'_0 = 1_4$
$B = 23_{\text{decimal}} = \langle B_2 B_1 B_0 \rangle_b = \langle 113 \rangle_4$
$A = 19_{\text{decimal}} = \langle A_2 A_1 A_0 \rangle_b = \langle 103 \rangle_4$

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

$$\begin{array}{r l}
x = \langle \mathbf{000} \rangle_4 & + \\
1011 & \quad A_0 B = 3_4 \cdot \langle 113 \rangle_4 = \langle 1011 \rangle_4 \\
\hline
1011 & + \\
123 & \quad t\,N = (N'_0 x_0 \bmod b)\,N = (1_4 \cdot 1_4 \bmod 4)_4\,\langle 123 \rangle_4 = \langle 123 \rangle_4 \\
\hline
1200 & \text{perform a right-shift of 1 digit} \Rightarrow \langle 120 \rangle_4 \\
 & \\
120 & + \\
000 & \quad A_1 B = 0 \cdot \langle 113 \rangle_4 = \langle 000 \rangle_4 \\
\hline
120 & + \\
000 & \quad t\,N = (N'_0 x_0 \bmod b)\,N = (1_4 \cdot 0_4 \bmod 4)_4\,\langle 123 \rangle_4 = \langle 000 \rangle_4 \\
\hline
120 & \text{perform a right-shift of 1 digit} \Rightarrow \langle 012 \rangle_4 \\
 & \\
012 & + \\
113 & \quad A_2 B = 1_4 \cdot \langle 113 \rangle_4 = \langle 113 \rangle_4 \\
\hline
131 & + \\
123 & \quad t\,N = (N'_0 x_0 \bmod b)\,N = (1_4 \cdot 1_4 \bmod 4)_4\,\langle 123 \rangle_4 = \langle 123 \rangle_4 \\
\hline
320 & \text{perform a right-shift of 1 digit} \Rightarrow \langle 032 \rangle_4 \\
 & \\
\mathbf{032}_4 &
\end{array}$$

$C{=}\langle 032 \rangle_4{=}14_{\mathrm{dec}}{<}N \Rightarrow C{=}19_{\mathrm{dec}}{\times}23_{\mathrm{dec}}{=}14_{\mathrm{dec}}{\in}(\mathbb{Z}_N,+,\times)$ (Montgomery domain)

Validation: $C{=}19_{\mathrm{dec}}{\times}23_{\mathrm{dec}} \overset{\mathrm{def}}{=} 19_{\mathrm{dec}} \cdot 23_{\mathrm{dec}} \cdot R^{-1} \bmod N \Rightarrow$
$C{=}19_{\mathrm{dec}} \cdot 23_{\mathrm{dec}} \cdot 19_{\mathrm{dec}} \bmod 27_{\mathrm{dec}}{=}8303_{\mathrm{dec}}{\equiv_{27_{\mathrm{dec}}}}14_{\mathrm{dec}}$