Cryptography and Architectures for Computer Security

Exam Code: 095947 (old 090959), A.Y. 2018–2019, Semester: 2

Prof. G. Pelosi

July 24th, 2019

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

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

Time: 2h, 15min. 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]

(a) An X.509 certificate for `foo.com` includes the 256 bit RSA public key for the aforementioned common name, and its MD5 hash signed with 512 bit RSA by Faust Certification Authority inc. Alice's browser contains a valid, trusted root CA certificate for Faust CA inc.

- Highlight which are Alice's concerns (all of them) toward the security of a possible TLS communication with foo.com, instantiated with the aforementioned X.509 certificate.

(b) A company is employing RIPEMD-64 hashes (64-bit digest) as an integrity checking mechanism for files on a disk. The security officer is currently concerned with the security margin against intentional replacement of files with garbage data and suggests to change the hashing mechanism to SHA-2-256. The commercial department points out that employing SHA-2-256 would increment the amount of required disk space and, to reduce the migration costs, proposes to employ SHA-2-256 to hash the file contents, and store only the first quarter of the digest for integrity checking.

- Is the security officer concern well justified? Provide a quantitative motivation to it.
- Is it possible to adopt the commercial department solution? Justify quantitatively the answer.

Solution:

(a)
- The first issue regarding the certificate is an insufficient keylength choice for both the RSA algorithms; anything below 2048-bit is to be considered insecure for RSA. The second concern is the fact that it is possible to find almost-arbitrary collisions to MD5 (i.e., the message is picked arbitrarily, save for the last MD5 block), which in turn allows to forge a certificate having the same signature as the one of `foo.com` even without passing by the CA.

(b)
- Yes: a 64 bit hash implies the possibility of obtaining a collision through exhaustive search in around 2^{32} operations, which is well within the realm of feasibility.

- No: performing the comparison only on the first 64 bits of the digest of SHA-2-256, and assuming that the bits of the first quarter of the hash follow the same uniform distribution as the rest of it, it is possible to obtain a partially colliding digest with the same computational effort of the previous hashing mechanism.

Question 2 [6 pts]
Consider the sequence $\{w_i\}_{i\geq 0} = \{s_i \oplus t_i\}_{i\geq 0}$, where: $\{s_i\}_{i\geq 0}$ is generated by the LFSR with characteristic[1] polynomial $1+x+x^2$, and
$\{t_i\}_{i\geq 0}$ is generated by the LFSR with characteristic polynomial $1+x+x^3$.

(a) What are the periods of $\{s_i\}_{i\geq 0}$ and $\{t_i\}_{i\geq 0}$?

(b) Draw the structure of the keystream generator corresponding to $\{w_i\}_{i\geq 0}$

(c) What are the possible periods of the sequence $\{w_i\}_{i\geq 0}$ and why?

Solution:

(a) Let us denote the characteristic polynomial of $\{s_i\}_{i\geq 0}$ and $\{t_i\}_{i\geq 0}$ as $G_S(x) = 1+x+x^2$ and $G_T(x) = 1+x+x^3$, respectively.
Their connection polynomials are: $C_S(x) = x^2+x+1$, $C_T(x) = x^3+x^2+1$.
Both connection polynomials must be considered in $\mathbb{F}_2[x]$ and it is easy to observe that they both have degree less or equal to 3 and no roots in $\mathbb{F}_2$, therefore both are irreducible and suitable to build a representation of the field $\mathbb{F}_{2^2}$ and $\mathbb{F}_{2^3}$, respectively.
Being $|\mathbb{F}^*_{2^2}| = 2^2-1 = 3$ a prime number, every element (except $\{0,1\}$) of the field is primitive (also the roots of $C_S(x)$).
This, in turn implies that $C_S(x)$ is primitive; Hence, the period of $\{s_i\}_{i\geq 0}$ is 3.
Being $|\mathbb{F}^*_{2^3}| = 7$ a prime number, every element (except $\{0,1\}$) of the field is primitive (also the roots of $C_T(x)$).
This, in turn, implies that $C_T(x)$ is primitive; Hence, the period of $\{t_i\}_{i\geq 0}$ is 7.

(b) see lectures ...

(c) `xor`ing the digits of the two keystreams (synchronously) it is easy to observe (e.g., with an example) that the period of the resulting keystream is $3\cdot 7 = 21$, that is the lowest common multiple of the two initial periods.

Question 3 [8 pts]
Consider the finite field $\mathbb{F}_{2^6}$.

(a) Establish if $f(x) = x^6+x^2+1 \in \mathbb{F}_2[x]$, $g(x) = x^6+x^3+1 \in \mathbb{F}_2[x]$ are irreducible and/or primitive polynomials.

(b) Let $\beta{=}\alpha{+}1$ be a generator of $\mathbb{F}^*_{2^6}$, where $\mathbb{F}_{2^6}{\cong}\mathbb{F}_2[x]/(g(x)){\cong}\mathbb{F}_2(\alpha)$, with $\alpha{\in}\{\mathbb{F}_{2^6}\backslash\mathbb{F}_2\}$ and $g(\alpha) = 0$. Show the generators of each subgroup of $(\mathbb{F}^*_{2^6}, \cdot)$.

(c) Compute the following discrete logarithm:
$m \equiv \log^{\mathsf{D}}_{\alpha+1}(\alpha^5+\alpha^2) \bmod |\alpha+1|$, applying the BSGS method.

[1] the *characteristic polynomial* $G(x)$ of an LFSR with length L is related to the *Connection polynomial*, $C(x)$, through the following relations: $G(x) = x^L C(x^{-1})$ and $C(x) = x^L G(x^{-1})$.

Solution:

(a) Given $f(x) = x^6 + x^2 + 1 \in \mathbb{F}_2[x]$, the algebraic structure $R = \mathbb{F}_2[x]/(f(x)) = \mathbb{F}(\alpha) = \{\theta_0 + \theta_1\alpha + \ldots + \theta_5\alpha^5 \mid \theta_i \in \mathbb{F}_2, f(\alpha) = 0\}$ is a field with $q = 64$ elements iif $\forall\ a \in R$ it is true that $a^q \equiv a$.
However, $\alpha^{64} \equiv (\alpha^6)^8 \cdot (\alpha^6)^2 \cdot \alpha^4 \equiv (\alpha^2+1)^8 \cdot (\alpha^2+1)^2 \cdot \alpha^4 \equiv (\alpha^{16}+1)\cdot(\alpha^8+\alpha^4) \equiv ((\alpha^6)^2 \cdot \alpha^4 + 1) \cdot (\alpha^6 \cdot \alpha^2 + \alpha^4) \equiv (\alpha^8 + \alpha^4 + 1) \cdot \alpha^2 \equiv (\alpha^4 + \alpha^2 + \alpha^4 + 1) \cdot \alpha^2 \equiv \alpha^4 + \alpha^2 \Rightarrow\ \alpha^{64} \not\equiv \alpha \Rightarrow$ not irreducible!

$f(x)$ is not irreducible, hence also not primitive (Indeed, $f(x) = (x^3 + x + 1)^2$).

Note that to test if a polynomial is primitive or not, the following conditions should hold: $\alpha^{\texttt{div}} \not\equiv 1$ with `div` a divisor of $2^6 - 1 = 63$ **AND** $\alpha^{64} \equiv \alpha$.

Let's apply an irreducibility test for $g(x) = x^6 + x^3 + 1$: $\gcd(g(x), x^{2^h} - x) =$ constant $\forall\ 1 \le h \le 3 \ldots$ it is true for every value of h, thus $g(x)$ is irreducible! Considering $g(x) = x^6 + x^3 + 1$ as a primitive polynomial and the field $\mathbb{F}_{2^6} \cong \mathbb{F}_2(\alpha)$, with $\alpha^6 \equiv \alpha^3 + 1$; the following conditions must be true:

$$\begin{cases} \alpha^3 \not\equiv 1 \Rightarrow \text{ true} \\ \alpha^7 \not\equiv 1 \Leftrightarrow\ \alpha^4 + \alpha \Rightarrow \text{ true} \\ \alpha^9 \not\equiv 1 \Leftrightarrow\ (\alpha^3+1)\cdot\alpha^3 \equiv \alpha^6 + \alpha^3 \equiv 1 \Rightarrow \text{ false} \\ \alpha^{21} \not\equiv 1 \Leftrightarrow\ \ldots \end{cases}$$

the polynomial $g(x) = x^6 + x^3 + 1$ is irreducible, but not primitive!

(b) $n = |\mathbb{F}^*_{2^6}| = 63 = 3^2 \cdot 7$, the subgroups can be listed as H_1, H_3, H_7, H_9, H_{21}, $H_{63} = \mathbb{F}^*_{2^6}$, where each subscript of the symbol H coincides with the cardinality of the subgroup itself: $|H_1| = 1$, $|H_3| = 3 \ldots$
A generator of H_1 is: 1;
A generator of H_3 is: $\beta^{n/3} = (\alpha+1)^{21}$;
A generator of H_7 is: $\beta^{n/7} = (\alpha+1)^{9}$;
A generator of H_9 is: $\beta^{n/9} = (\alpha+1)^{7}$;
A generator of H_{21} is: $\beta^{n/21} = (\alpha+1)^{3}$;
A generator of H_{63} is: $\beta = (\alpha+1)$.

(c) $n = |\alpha + 1| = 63$, $g(x) = x^6 + x^3 + 1$, $g(\alpha) = 0$, $\alpha \in \{\mathbb{F}_{2^6} \setminus \mathbb{F}_2\}$

$$(\alpha+1)^j \overset{?}{\equiv} (\alpha^5 + \alpha^2) \cdot \left((\alpha+1)^{-\lceil\sqrt{n}\rceil}\right)^i,\ i, j \in \{0, \ldots, \lceil\sqrt{n}\rceil\}$$

$$(\alpha+1)^{-\lceil\sqrt{n}\rceil} \equiv (\alpha+1)^{-8} \equiv ((\alpha+1)^8)^{-1} \equiv (\alpha^8+1)^{-1} \equiv (\alpha^5 + \alpha^2 + 1)^{-1} \equiv$$
$$\equiv \ldots \text{ extended Euclidean Alg. } \ldots = \alpha^5 + \alpha^4 + \alpha^3 + 1.$$

$$\text{BabyStep} \overset{?}{\equiv} \text{GiantStep} \ \Leftrightarrow (\alpha+1)^j \overset{?}{\equiv} (\alpha^5 + \alpha^2) \cdot \left(\alpha^5 + \alpha^4 + \alpha^3 + 1\right)^i$$

Baby step table:

j	0	1	2	3	4	5	6	7
$(\alpha+1)^j$	1	$\alpha+1$	α^2+1	$\alpha^3+\alpha^2+\alpha+1$	α^4+1	$\alpha^5+\alpha^4+\alpha+1$	$\alpha^4+\alpha^3+\alpha^2$	$\alpha^5+\alpha^2$

It is easy to see that $j = 7$, $i = 0$(Giant Step), thus $m = 7$.

Question 4 [6 pts]
Explain briefly why elliptic curve based cryptosystems usually provide shorter keys with respect to RSA or discrete log systems employing a modular integer arithmetic.
Consider the elliptic curve $y^2 = x^3 + 6x + 3$ over $\mathbb{Z}_{11}$

(a) How many points lie on it ?

(b) What is the sum of the points (4, 5) and (5, 9)?

Solution:
see lectures . . .

x, y	0	1	2	3	4	5	6	7	8	9	10
$(x^3 + 6x + 3)$ mod 11	3	10	1	4	3	4	2	3	2	5	7
y^2 mod 11	0	1	4	9	5	3	3	5	9	4	1

. . .
$n = |\mathbb{E}(\mathbb{Z}_{11})| = 15$
(4, 5)+(5, 9) = . . . = (7, 5)

Question 5 [6 pts]

(a) Apply the Pollard's ρ method to factorize the RSA modulus $n = p \cdot q = 713$.
Assume $f(x) = x^2 + 1 \bmod n$ as "random-walking" function.
Show every step of the computation.
(As a backup alternative, apply a "trivial division" strategy).

(b) Choose an admissible public exponent e between the values $e = 11_{\mathtt{dec}}$ and $e = 13_{\mathtt{dec}}$ and compute the value of the corresponding RSA private key $k_{priv} = (p, q, \varphi(n), d)$. Show every step of the computation.

(c) Sign the message m=$100_{\mathtt{dec}} \in \mathbb{Z}_n$ (without employing any padding scheme) through applying the CRT. Describe each step of the procedure.

Solution:

(a) see lectures . . ., $n = 713$, $p = 23$, $q = 31$.

(b) $\varphi(n) = 660 = 2^2 \cdot 3 \cdot 5 \cdot 11$;
$gcd(\varphi(n), e) = 1 \Rightarrow e = 13$;
$d = 13^{-1} \bmod 660 = 13^{159} \bmod 660 = \ldots = 457$.

(c) $s \equiv_{713} 100^{457} \Leftrightarrow \begin{cases} s \equiv_{23} 100^{457 \bmod 22} \\ s \equiv_{31} 100^{457 \bmod 31} \end{cases} \Leftrightarrow \begin{cases} s \equiv_{23} 8^{17} \\ s \equiv_{31} 7^{7} \end{cases} \ldots$
$\ldots\ s \equiv_{713} 59.$

Question 6 [6 pts]
Consider a school-book implementation of the RSA encryption function with $k_{\mathtt{pub}}$=$\langle 3, n\rangle$, n=3×17; employing the Montgomery arithmetics primitive $\mathtt{MMul}_n(\cdot,\cdot)$.

(a) Write the pseudo-code of an encryption primitive (employing the $\mathtt{MMul}_n(\cdot,\cdot)$) taking as input the public key and a plaintext message in the integer domain.

(b) Show the value $\widetilde{m}$ of m=42 $\in \mathbb{Z}_n$ in the Montgomery domain, assuming the smallest value of the Montgomery radix, and show the computation of $\widetilde{m^2} = \texttt{MMul}_n(\widetilde{m}, \widetilde{m})$ assuming a binary encoding of $\widetilde{m}$.

(c) Show the value of $\widetilde{c}$=$\texttt{MMul}_n(\widetilde{m^2}, \widetilde{m})$ and the corresponding value of the ciphertext c in the integer domain.

Solution:

Algorithm 1: Schoolbook-RSAenc

```
Input: $m$, plaintext message; $e$, public exponent; $n$, public modulus
Output: $c$, ciphertext
$t \leftarrow \lceil \log_2 e \rceil$
$\texttt{R} \leftarrow 2^{\lceil \log_2 n \rceil}$
$\texttt{Rsquared} \leftarrow \texttt{R}^2 \bmod n$ // as $n < \texttt{R} < 2n$, ...  with schoolbook mul and substractions
$\widetilde{m} \leftarrow \texttt{MMul}_n(m, \texttt{Rsquared})$
$\widetilde{c} \leftarrow \widetilde{m}$
for $i \leftarrow t - 2$ downto 0 do
    $\widetilde{c} \leftarrow \texttt{MMul}_n(\widetilde{c}, \widetilde{c})$
    if $e_i == 1$ then
        $\widetilde{c} \leftarrow \texttt{MMul}_n(\widetilde{c}, \widetilde{m})$
$c \leftarrow \texttt{MMul}_n(\widetilde{c}, 1)$
return $c$
```

(a) see Algorithm 1.

(b) $R = 64$; $R^2 \bmod n = 16$.
$R' = R^{-1} \bmod n \equiv_{51} 64^{-1} \equiv_{51} 13^{-1} \equiv_{51} 4$.
$\widetilde{m} = m \cdot R \bmod n = 42 \cdot 64 \bmod 51 = 36$.
This is equivalent to compute $\widetilde{m} = \texttt{MMul}_n(m, R^2 \bmod n) \equiv_{51} 42 \cdot 16 \cdot 4 \equiv_{51} 36$.
see lectures for the computation of $\widetilde{m^2} = \texttt{MMul}_n(\widetilde{m}, \widetilde{m})$ employing a binary encoding of the operands ... $\widetilde{m^2} = \texttt{MMul}_n(\widetilde{m}, \widetilde{m})$= $36^2 \cdot 4 \equiv_{51} 33$.

(c) $\widetilde{c} = \texttt{MMul}_n(\widetilde{m^2}, \widetilde{m}) = ((33 \cdot 36 \cdot 4) \bmod 51) \equiv_{51} 9$.
$c = \texttt{MMul}_n(\widetilde{c}, 1) = 9 \cdot 1 \cdot 4 \equiv_{51} 36$.