Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

"Digital signature schemes"

Proposed exercises

Exercise 1:

Consider an RSA system with p=13 and q=19. We want to sign the message M=10. If the exponent of our public key is e=11, compute the digital signature of M and verify it.

Solution:

The conditions are:

$N=p\cdot q=13\cdot 19=247$

$\phi(N)=12\cdot 18=216$

$1<e<N \rightarrow 1<11<247$ True

GCD $(e, \phi(N)) = 1 \rightarrow$ GCD $(11, 216)=1$ True

p y q are not large primes but we will use them anyway

First we calculate the private key of the signer:

$d\cdot e=1 \bmod (\phi(N))$

$11\cdot d=1 \bmod (216)$

$216=19\cdot 11+7$	$7=216-19\cdot 11$
$11=1\cdot 7+4$	$4=11-1\cdot 7$
$7=1\cdot 4+3$	$3=7-1\cdot 4$
$4=1\cdot 3+1$	$1=4-1\cdot 3$

$1=4-1\cdot 3 \bmod (216) = 4-(7-1\cdot 4) \bmod (216) = 2\cdot 4-7 \bmod (216) =$

$= 2\cdot(11-1\cdot 7)-7 \bmod (216) = 2\cdot 11-3\cdot 7 \bmod (216) = 2\cdot 11-3\cdot(216-19\cdot 11) \bmod (216) =$

$= 59\cdot 11-3\cdot 216 \bmod (216) = 59\cdot 11 \bmod (216)$

$d = 59$

The signature is:

$F(M)=M^d \bmod (N)=10^{59} \bmod (247)=(10^3)19\cdot 10^2 \bmod (247)=12^{19}\cdot 10^2 \bmod (247)=$

$=4^{19}\cdot 3^{19}\cdot 10^2 \bmod (247)=4^3\cdot(3^2)^4\cdot 3^{19}\cdot 10^2 \bmod (247)=4^3\cdot 3^{27}\cdot 10^2 \bmod (247)=$

$=4^3\cdot 3^2\cdot(-4)5\cdot 10^2 \bmod (247)=(-1)\cdot 4^8\cdot 3^2\cdot 10^2 \bmod (247)=(-1)\cdot(9)^2\cdot 3^2\cdot 10^2 \bmod (247)=$

$=(-1)\cdot 3^6\cdot 10^2 \bmod (247)=(-1)\cdot 3\cdot(-4)\cdot 100 \bmod (247)=4\cdot 53 \bmod (247)=212 \bmod (247)$

Signature verification:

$F^e \bmod (N)=212^{11} \bmod (247)$

$212\cdot 212=44944$; $44944 \bmod 247=237 \bmod 247=(-10) \bmod 247$

$212^{11} \bmod (247)=(-10)^5\cdot 212 \bmod (247)=(-1)\cdot 100\cdot 1000\cdot 212 \bmod (247)=$

$=(-1)\cdot 100\cdot 12\cdot 212 \bmod (247)=(-1)\cdot 10\cdot 10\cdot 12\cdot 2\cdot 106 \bmod (247)=$

$=(-1)\cdot 10\cdot 240\cdot 106 \bmod (247)=(-1)\cdot 10\cdot(-7)\cdot 106 \bmod (247)=10\cdot 7\cdot 53\cdot 2 \bmod (247)=$
$=10\cdot 2\cdot 371 \bmod (247)=10\cdot 2\cdot 124 \bmod (247)=10\cdot 248 \bmod (247)=10$

Exercise 2:

Two spies A and B exchange messages by email. They want to keep in secret these messages and also authenticate the origin, because A suspects that C wants to impersonate B. Accordingly, A and B digitally sign and encrypt their emails coded with 27 elements (A=00, B=01 ,…, Ñ=14 ,..., Z=26). They use RSA both to sign and encrypt with the following parameters.

A: $N_A= 3 \cdot 13 =39$ $e_A=5$

B: $N_B=5 \cdot 11 = 55$ $e_B=9$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

A and B has a plan and they only need to know if the city where they want to meet is PARIS (P) or LISBOA (L). They encrypt the first and the second letter of the city and only sign the first. Consider the city for A is Paris and for B is Lisboa.

a) Calculate the two messages encrypted: C_A y C_B.

b) To sign the messages. $F_A(M_A)$ y $F_B(M_B)$.

c) Decrypt the ciphertexts and verify the signatures

d) A and B do not agree in the city. Indicate a secure protocol where they only exchange the message PARIS

Solution:

a) Message from A to B is:

$M_A=[PA]=(16,0)$

$C_A = M_{A1}^{eB} \pmod{N_B}$, $M_{A2}^{eB} \pmod{N_B} = 16^9, 0^9 \bmod 55 =$

$= 2^{36}, 0 \pmod{55} = 9^6, 0 \pmod{55} = 3^{12}, 0 \pmod{55} = (3^4)^3 \pmod{55} = 26^3, 0 \pmod{55} =$

$16\cdot 26, 0 \pmod{55} = [\mathbf{31, 0}] \pmod{55}$

Message from B to A is:

$M_B=[\ LI\ ]=(11,8)$

$C_B = M_{B1}^{eA} \pmod{N_A}$, $M_{B2}^{eA} \pmod{N_A} = 11^5, 8^5 \pmod{39} = (11^2)^2\cdot 11, (2^5)^3 \pmod{39} = 4^2\cdot 11, (-7)^3 \pmod{39} = 4\cdot 5, 10\cdot(-7) \pmod{39} = [\mathbf{20, 8}] \pmod{39}$

b) First we need to calculate the private keys, and for this, $\phi(N)$:

$\phi(N_A)=2\cdot 12=24$

$\phi(N_B)=4\cdot 10=40$

$e_A\cdot d_A=1 \pmod{\phi(N_A)}$; $d_A\cdot 5=1 \pmod{24} \rightarrow d_A=5$

$e_B\cdot d_B=1 \pmod{\phi(N_B)}$; $d_B\cdot 9=1 \pmod{40} \rightarrow d_B=9$

Now the signatures:

$F_A(M_A)=P^{dA} \pmod{N_A}=16^5 \pmod{39}=7^4 \pmod{39}=22 \pmod{39}$

$F_B(M_B)=L^{dB} \pmod{N_B}=11^9 \pmod{55}=11 \pmod{55}$

Note:
A sends (C_{1A}, C_{2A}, F_A) = (31,0,22)
B sends (C_{1B}, C_{2B}, F_B) = (20,8,11)

c) B decrypts the message sent by A:
$M_A=C_{1A}^{dB}(\text{mod } N_B)$,C_{2A}^{dB} (mod N_B)=31^9, 0^9 mod (55)=16 ,0(mod 55)=PA

B verifies A's signature:
F_A^{eA}mod (N_A)=22^5 (mod 39)=16^2·22(mod 39)=22·22(mod 39)=16(mod 39)=P

A decrypts the message sent by B:
$M_B=C_{1B}^{dA}(\text{mod } N_A)$,C_{2B}^{dA}(mod N_A)=20^5,8^5 (mod 39)=11,8 (mod 39)=LI

A verifies B's signature:
F_B^{eB} mod (N_B)=11^9(mod 55)=11(mod 55)=L

d) A simple solution would be: A sends PARIS encrypted and signed to B. B verifies the signature and decrypts it returning to A the message PARIS encrypted and signed by him. A verifies the signature and decrypts the message. A sends an acknowledgement to B.

Exercise 3:
Calculate and verify the El Gamal signature of a message M=5, g=2, p=11, X_A=8 (signer's private key), and the random number k=9.

Solution:

g is generator of Z p
1<X_A<p−1 → 1<8<10 → OK
1<k<p−1 → 1<9<10 → OK
gcd(9,10) = 1 → OK
r=g^k (mod p)=2^9 (mod 11)=512(mod 11)=6(mod 11)

M =X_A·r+k·s (mod p−1) → 5=8·6+9·s mod (10) → 5=8+9·s mod (10) → 5=8−s → **s=3**

::::::::::::::::::::::::::::ALTERNATIVE:::::::::::::: ::::::::::::::
M =X_A·r+k·s(mod p−1) → 5=8·6+9·s mod (10) → 5=8+9·s → −3=9·s(mod 10)

7=9·s(mod 10)

Variable change z=s / 7 (mod 10)
7=9·z·7(mod 10) ;1=9·z (mod 10)=(−1)·z (mod 10) → **z=−1=9** mod (10)
s=7·z (mod 10)=7·9(mod 10)=**3**(mod 10)

:::::::::::::::::::::::::::: :::::::::::::: :::::::::::::::: :::::::::::::: :::::::::::::::: ::::::::::::::::

Sender sends (M,r,s): (5,6,3)

Signature verification:
$V_1=Y_A^r \cdot r^s \pmod p$;
$Y_A=g^{X_A} \pmod p=2^8 \pmod{11}=256 \pmod{11}=3 \bmod (11)$
$V_1=Y_A^r \cdot r^s \pmod p=3^6 \cdot 6^3 \pmod{11}=3^9 \cdot 2^3 \pmod{11}=(-1) \cdot 3^{10} \pmod{11}=(-1) \cdot (-2)^5 \pmod{11}=$
$=32 \pmod{11}=10$

$V_2=g^M \pmod p=2^5 \pmod{11}=10$

As $V_1 == V_2$, the signature is valid.

Exercise 4:
Alice wants to send to Bob a message M composed of hexadecimal digits, using a signature with appendix. She uses El Gamal with the hash function o-exclusive (⊕), x ⊕ y = (x+y) mod 16, where x and y are hexadecimal digits. If M is

0 1 2 3 4 5 6 7 8 9 A B C D E F

a) Apply the hash function to get the message-digest R that is a hexadecimal digit long

b) If A chooses, p=17, g=7, X_A=5, Y_A=11, k=9 Does these parameters satisfy the conditions to be used in El Gamal signature algorithm?

c) Get the signature on message M.

d) Make the calculations that B does in order to verify the integrity of the message received. Is the signature valid?

Solution:

a) Alice calculates: 0⊕1⊕ 2⊕3⊕ 4⊕ 5⊕ 6⊕ 7⊕ 8⊕ 9⊕ A⊕ B⊕ C⊕ D⊕ E⊕ F.
0+1+2+3+4+5+6+7+8+9+A+B+C+D+E+F=120
0⊕1⊕ 2⊕3⊕ 4⊕5⊕6⊕7⊕8⊕9⊕ A⊕ B⊕C⊕ D⊕ E⊕ F=120(mod 16)=8

b) • p is prime (but not large enough)
• g is generator mod p because:
$7^0 \bmod 17=1$; $7^1 \bmod 17=7$; $7^2 \bmod 17=15$; $7^3 \bmod 17=3$; $7^4=4$; $7^5=11$; $7^6=9$; $7^7 \bmod 17=12$;
$7^8 \bmod 17=16$; $7^9 \bmod 17=10$; $7^{10}=2$; $7^{11}=14$; $7^{12}=13$; $7^{13}=6$; $7^{14}=8$; $7^{15}=5$
• X_A 1 < 5 < 16
• k 1 < 9 < 16 and gcd(9,16) = 1

c) $r=g^k \pmod p=7^9 \pmod{17}=10$
$H(M)=X_A \cdot r+k \cdot s \bmod (p-1)$ → $8=5 \cdot 10+9 \cdot s \pmod{16}$; $8=2+9 \cdot s \pmod{16}$; $6=9 \cdot s \pmod{16}$
$z= s/6 \pmod{16}$ → $1=9 \cdot z \pmod{16}$ → z=9
$s = 9 \cdot 6 \pmod{16} = 6 \pmod{16}$
(M,r,s) = (**0 1 2 3 4 5 6 7 8 9 A B C D E F**,10,6)

d) $Y_A=g^{X_A} \pmod p=7^5 \pmod{17}=15 \cdot 15 \cdot 7 \pmod{17}=8 \cdot 12 \pmod{17}=-6 \pmod{17}=11$

$V_1 = Y_A^r \cdot r^s \pmod p = 11^{10} \cdot 10^6 \pmod{17} = 2^5 \cdot (-2)3 \pmod{17} = (-1) \cdot 2^8 \pmod{17} = 16 \pmod{17}$
$V_2 = g^{H(M)} \pmod{17} = 7^8 \pmod p = 16$

Signature is valid.