Exam TMA4160 Cryptography
Suggested solutions

December 14, 2017

Problem 1

Notation: For arithmetic modulo 271, we omit the modulus.

a. Let $a = \log_g x$. The given equation tells us that

$$147 + 3a \equiv 0 \pmod{270} \qquad \text{or} \qquad 3a \equiv -147 \equiv 123 \pmod{270}.$$

Note that 3 is not invertible modulo 270, but since 270 divides the difference between $3a$ and 123, 90 must divide the difference between a and 41, or

$$a \equiv 41 \pmod{90}.$$

We know that the only possible values for $\log_g x$ are 41, 131 and 221.

Note that if the answers we get in the next two problems are not one of these three, we know that something is wrong.

b. It is easy to see that $270 = 2 \cdot 3^3 \cdot 5$, so we need to compute $a = \log_g x$ modulo 2, 3^3 and 5.

Modulo 2: $270/2 = 135$, so

$$g^{135} \equiv -1 \equiv 270 \qquad \text{and} \qquad x^{135} \equiv 270$$

which means that $a \equiv 1 \pmod{2}$.

Modulo 5: $270/5 = 54$, so

$$g^{54} \equiv 10 \qquad \text{and} \qquad x^{54} \equiv 10$$

which immediately means that $a \equiv 1 \pmod{5}$.

Modulo 3^3: $270/3^3 = 10$, so

$$g^{10} \equiv 114 \qquad \text{and} \qquad x^{10} \equiv 83.$$

So we need to compute $\log_{114} 83 \equiv a \pmod{27}$. We begin by computing

$$114^9 \equiv 242 \qquad \text{and} \qquad (114^9)^2 \equiv 28.$$

Then

$$83^9 \equiv 28 \qquad \Rightarrow \qquad a \equiv 2 \pmod 3.$$

Next

$$(83/114^2)^3 \equiv 106^3 \equiv 241 \qquad \Rightarrow \qquad a \equiv 2 + 1 \cdot 3 \pmod 9.$$

Finally

$$106/(114^3)^1 \equiv 242 \qquad \Rightarrow \qquad a \equiv 2 + 1 \cdot 3 + 1 \cdot 3^2 \equiv 14 \pmod{27}.$$

Chinese Remainder Theorem: We have

$$\begin{aligned} a &\equiv 1 \pmod 2 \\ a &\equiv 14 \pmod{27} \\ a &\equiv 1 \pmod 5 \end{aligned}$$

An easy computation tells us that $a \equiv 41 \pmod{270}$, which means that $\log_g x = a = 41$.

c. We choose $L = 16 \approx \sqrt{270}$, and compute the (unsorted) table

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
g^i	1	6	36	216	212	188	44	264	229	19	114	142	39	234	49	23

We find that $g^{16} \equiv 138$, so we shall multiply by $138^{-1} \equiv 163$, and find that

$$\begin{aligned} 51 \cdot 163 &\equiv 183 \\ 183 \cdot 163 &\equiv 19 \equiv g^9 \end{aligned}$$

so $x g^{-16 \cdot 2} \equiv g^9$, which means that $\log_g x \equiv 16 \cdot 2 + 9 \equiv 41$, which means that $\log_g x = 41$.

Problem 2

a. Sinse $4P$ is given, there are two sensible ways to check that $5P + 2R = \mathcal{O}$: We can compute $4P + P = (8, 10)$ and $R + R = (8, 9)$ and observe that they are inverses, or compute $(4P + P) + R = (14, 11)$ and observe that it is an inverse of R. Either way works. (The first method uses both variants of the addition formula, in the second method both additions are of distinct points.)

b. We get that $7 + 3\log_P R + 4\log_P Q \equiv 0 \pmod{23}$. From the previous problem, we have that $5 + 2\log_P R \equiv 0 \pmod{23}$. This gives us

$$0 \equiv 14 + 6\log_P R + 8\log_P Q - 15 - 6\log_P R \equiv 8\log_P Q - 1 \qquad \Rightarrow \qquad \log_P Q = 3.$$

Problem 3

a. Modulo n, we get that

$$\sigma \equiv \tau^e / r^e \equiv (t^d)^e / r^e \equiv (r^e h(m))^{de} / r^e \equiv r^e h(m) / r^e \equiv h(m).$$

So σ is a valid signature on m.

Bob sees t. The map $x \mapsto x^e \bmod n$ is a bijection, which means that if r is equally likely to be any invertible number, so is $r^e \bmod n$. And multiplication by an invertible random number is an invertible map. So if $r^e \bmod n$ is equally likely to be any invertible number, so is $r^e h(m) \bmod n$ as long as $h(m)$ is invertible modulo n.

We may safely assume that $h(m)$ is invertible for any m Alice comes up with, so from Bob's point of view, regardless of what m is, t will be an invertible number chosen at random, and therefore it will be independent of m.

It follows that Bob learns nothing.

b. We consider elements relatively prime to n. (Order does not make sense for elements not relatively prime to n.)

An element x is a square if there exists a z such that $z^2 \equiv x \pmod{n}$. But then modulo p we have that

$$x^{(p-1)(q-1)/4} \equiv (z^2)^{(p-1)(q-1)/4} \equiv (z^{p-1})^{(q-1)/2} \equiv 1 \pmod{p}.$$

The same holds modulo q, and the claim follows.

Note that $(p-1)(q-1)/4$ is an odd number, so let d be an inverse of 2 modulo $(p-1)(q-1)/4$. Let x be a square. Then

$$(x^d)^2 \equiv x^{2d} \equiv x \pmod{n}$$

so $x^d \bmod n$ is a square root of x.

Since Bob knows p and q, he can easily compute d using (for example) the Extended Euclidian algorithm, and then he can compute $x^d \bmod n$ using any fast exponentiation algorithm (such as square and multiply).

c. Note that since x has Jacobi symbol 1 over n, x has the same Legendre symbol over both p and q. Furthermore, since $(p-1)/2$ and $(q-1)/2$ are both odd, -1 is a non-square for both p and q. It follows that -1 has Jacobi symbol 1.

If x is a square, we are done. If x is a non-square, then x is a non-square modulo both p and q. But $-x$ is then a square modulo both p and q. From which it follows (for example by CRT) that $-x$ is a square modulo n.

d. We get that

$$\sigma^2 \equiv \tau^2 / r^2 \equiv \pm t / r^2 \equiv \pm r^2 h_n(m) / r^2 \equiv \pm h_n(m) \pmod{n}.$$

So σ is a valid signature on m.

Alice chooses some r with Jacobi symbol -1. She computes $t = r^2 \bmod n$ and sends t to Bob. Bob returns τ such that $\tau^2 \equiv \pm t \equiv \pm r^2 \pmod{n}$. Since their Jacobi symbols are different, we know that $r \not\equiv \pm\tau \pmod{n}$, so $\gcd(r-\tau, n)$ is either p or q.

Problem 4

Suppose Alice's messages are two bits long. The first message is (m_1, m_2), the second is $(1-m_1, 1-m_2)$. Which means that the first signature is (say) (a_{1,m_1}, a_{2,m_2}), and the second signature is $(a_{1,1-m_1}, a_{2,1-m_2})$.

Eve can now create a valid signature $(a_{1,m_1}, a_{2,1-m_2})$ on the message $(m_1, 1-m_2)$.