Exam TMA4160 Cryptography
Suggested solutions

December 16, 2015

Problem 1

The number $n = 2465$ is trivially divisible by 5, but we do not use this fact here.

a. Since we need to compute $3^{(n-1)/4} \bmod n$ later on, it makes sense to compute it first and then square the result. Note that $616 = 2^9 + 2^6 + 2^5 + 2^3$. We compute:

$$
\begin{aligned}
3^{2^1} \bmod n &= 9 \\
3^{2^2} \bmod n &= 9^2 \bmod n = 81 \\
3^{2^3} \bmod n &= 81^2 \bmod n = 1631 \\
3^{2^4} \bmod n &= 1631^2 \bmod n = 426 \\
3^{2^5} \bmod n &= 426^2 \bmod n = 1531 \\
3^{2^6} \bmod n &= 1531^2 \bmod n = 2211 \\
2^{2^7} \bmod n &= 2211^2 \bmod n = 426 \\
2^{2^8} \bmod n &= 426^2 \bmod n = 1531 \\
2^{2^9} \bmod n &= 1531^2 \bmod n = 2211
\end{aligned}
$$

Then we compute:

$$
\begin{aligned}
3^{2^9+2^6+2^5+2^3} &= 1631 \cdot 1531 \cdot 2211 \cdot 2211 \bmod n \\
&= 1631 \cdot 1531 \cdot 426 \bmod n = 1886.
\end{aligned}
$$

Finally,

$$1886^2 \bmod n = 1.$$

We did 10 modular multiplications. (The two lines in red above did not require computation.)

(The problem statement suggests that $3^{1232} \bmod n$ and $3^{616} \bmod n$ should be computed separately, which requires one more multiplication. Saving that multiplication is allowed, even if not entirely in accordance with the problem statement.)

b. We note that $n \equiv 1 \pmod 4$, and compute

$$\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

We know that if n is prime, then

$$3^{(n-1)/2} \equiv \left(\frac{3}{n}\right) \pmod n,$$

from which it follows that n is not prime.

c. We already computed $3^{(n-1)/4} \bmod n = 1886$ above.

We know that $1886^2 \equiv 1 \equiv (-1)^2 \pmod n$, but $1886 \not\equiv \pm 1 \pmod n$, so n divides the difference between the squares, but not $1886 - 1$. We compute

$$\begin{aligned} 2465 &= 1 \cdot 1885 + 580 \\ 1885 &= 3 \cdot 580 + 145 \\ 580 &= 3 \cdot 145 \end{aligned}$$

We know that 145 is a proper factor of n.

We did 3 integer divisions.

Problem 2

a. We compute $2P, 3P, \ldots$ until we find Q. Since the logarithm is small, this is faster than using a more sophisticated algorithm.

$2P$:

$$\begin{aligned} \lambda &= \frac{3 \cdot 62^2 + 1}{2 \cdot 15} = 78 \cdot 29 = 50 \\ x_3 &= 50^2 - 62 - 62 = 6 \\ y_3 &= 50(62 - 6) - 15 = 20 \end{aligned}$$

$3P = 2P + P$:

$$\begin{aligned} \lambda &= \frac{20 - 15}{6 - 62} = \frac{5}{23} = 5 \cdot 55 = 38 \\ x_3 &= 38^2 - 62 - 6 = 33 \\ y_3 &= 38(6 - 33) - 20 = 60 \end{aligned}$$

We observe that this is $-Q$, but we do not (yet) know the order of P.

$4P = 3P + P$:

$$\lambda = \frac{15 - 60}{62 - 33} = -45 \cdot 30 = 7$$
$$x_3 = 7^2 - 33 - 62 = 33$$
$$y_3 = 7(33 - 33) - 60 = 19$$

This is Q, so $\log_P Q = 4$.

We needed 10 modular multiplications, using two of the three hints.

b. We know that the order of P is 7, since we observed $3P = -4P$.

Alternatively, if we did not compute $3P$ in the previous problem, but computed $2P$ and $4P$, we could use the information given, namely that the order is either $3P$, $5P$ or $7P$. We observe that $2P \neq -P$ and $4P \neq -P$, which leaves 7 as the only possible order.

If we also know that there is a point R on E of order 11, we know that the number of rational points on E must be divisible by 7 and 11. Hasse's theorem then says that the number of points on the curve is 77.

c. Suppose $T = aS$. It is important to remember that the group order is 77.

Since $11S = P$ and $11T = Q$, we get that $4P = Q = 11aS = a \cdot (11S) = aP$, which means that $a \equiv 4 \pmod 7$.

Since $7S = 3R$ and $7T = 8R$, we get that $8R = 7aS = a \cdot (7S) = a \cdot (3R) = 3aR$, which means that $3a \equiv 8 \pmod{11}$. Multiplying both sides by 4 (an inverse of 3 modulo 11), we get $a \equiv 10 \pmod{11}$.

The Chinese remainder theorem then tells us that $a \equiv 32 \pmod{77}$, so $\log_S T = 32$.

Problem 3

a. We know that B and B' both generate the same lattice. Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be the rows of B, and let $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$ be the rows of B'. Note that these are all in the lattice.

Now, for every i, since $\mathbf{b}_i$ is in the lattice, there is an integer linear combination of the vectors $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$ that equals $\mathbf{b}_i$. In other words, there is an integer vector $\mathbf{c}_i$ such that $\mathbf{c}_i B' = \mathbf{b}_i$. If we let $\mathbf{c}_1, \ldots, \mathbf{c}_n$ be the rows of a matrix C, we get that $CB' = B$.

In the same way, we get an integer matrix D such that $DB = B'$. Then $CDB = B$, and since B is invertible, $CD = I$. It follows that C and D are invertible integer matrices.

b. All that is non-trivial is to show that the scheme decrypts correctly. Suppose the ciphertext is $(\mathbf{x}, w)$ where $\mathbf{x}$ is $\mathbf{a}B' + \mathbf{e}$ with $||\mathbf{e}|| < \delta$. We only need to show h is applied to the same values.

We know that $\mathbf{a}B' = \mathbf{a}UB$ is the lattice point closest to $\mathbf{x}$. By assumption, we have that $\lfloor \mathbf{x}B^{-1} \rceil B = \mathbf{a}UB$. Multiplying by $B^{-1}U^{-1}$ from the right gives us that $\mathbf{a} = \lfloor \mathbf{x}B^{-1} \rceil U^{-1} = \mathbf{d}$. It is then clear that $\mathbf{e} = \mathbf{x} - \mathbf{d}UB$.