ELEMENTARY NUMBER THEORY AND CRYPTOGRAPHY II
SOLUTIONS FOR PROBLEM SHEET 5
MICHAELMAS TERM 2014

(1) (a) By taking the first few exponents, we find

$$15^3 \equiv 15^2 \cdot 15 = 225 \cdot 15 = 23 \cdot 15 = 345 \equiv 42 \pmod{101}$$

and

$$15^4 = 15^3 \cdot 15 \equiv 42 \cdot 15 = 630 \equiv 24 \pmod{101}.$$

Therefore we derive $m = 3$ and $n = 4$.
Hence we can find the shared secret key

$$(15^3)^4 \equiv 42^4 = (42^2)^2 = 1764^2 \equiv 47^2 \equiv 2209 = 2121 + 88 \equiv 88 \pmod{101}.$$

(b) One way has given in part (a) above, the second one is by

$$(15^4)^3 \equiv 24^3 \equiv 576 \cdot 24 \equiv 71 \cdot 24 \equiv -30 \cdot 24 = -720 \equiv -13 \equiv 88 \pmod{101}.$$

(2) If we have a message given as a number $m \pmod{31}$ and encrypt using the encryption exponent $e = 7$, then we find a decryption exponent by writing

$$e \cdot x + \varphi(m)y = 1$$

for some integers x and y, e.g. from (a) we find $x = 13$ and $y = -3$ do it. Therefore the inverse map of $E(x) = x^7 \pmod{31}$ is given by $E^{-1}(y) = x^{13} \pmod{31}$.

(3) Factorization of n gives $114113 = 113 \cdot 101$ (one can find it either by Fermat method or by trial and error). Therefore we have $\varphi(11413) = 11200$ and we can take the decryption exponent $d = 3$ since $3 \cdot 7467 \equiv 1 \pmod{11200}$. Computing $5859^3 \pmod{11413}$ gives the message $X = 1415$.

(4) According to the lectures, the two primes are the roots of the polynomial

$$(x - p)(x - q) = x^2 - (n - \varphi(n) + 1)x + n = x^2 - 1332x + 442931,$$

which we can solve easily as

$$x = 666 \pm \sqrt{666^2 - 442931} = 666 \pm 25,$$

and so $n = pq = (666 - 25) \cdot (666 + 25) = 641 \cdot 691$.

(5) (a) For p and q odd primes and $n = pq$ we have that $\varphi(n) = (p-1)(q-1)$. For a coprime to pq have

$$a^{p-1} \equiv 1 \pmod{p}, \qquad a^{q-1} \equiv 1 \pmod{q}$$

by Fermat, and so (by raising to the power $(q-1)/2 \in \mathbb{Z}$ and $(p-1)/2 \in \mathbb{Z}$, respectively) we find

$$(a^{p-1})^{\frac{1}{2}(q-1)} \equiv 1 \pmod{p}, \qquad (a^{q-1})^{\frac{1}{2}(p-1)} \equiv 1 \pmod{q},$$

and putting these two together we obtain indeed

$$a^{\frac{1}{2}(p-1)(q-1)} = a^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{n}.$$

(b) Let d and e be integers with $de \equiv 1 \pmod{\frac{1}{2}\varphi(n)}$. Then $a^{de-1} \equiv 1 \pmod{n}$ by the above (raise to the integer power $(de-1)/(\frac{1}{2}\varphi(n))$).

(6) (a) Fermat factorization algorithm for $n = 3525283$ chekcs $x = \lceil\sqrt{n}\rceil + j$ for $j = 0, 1, 2, \ldots$ and to check numerically if $\sqrt{x^2 - n}$ is an integer. We obtain for $j = 0, 1, 2, 3, 4$ the following respective values

$$40.012\ldots, \quad 73.198\ldots, \quad 95.482\ldots, \quad 113.481\ldots, \quad 129.000\,.$$

That is, $1882^2 - n = 129^2$ and so $n = (1882-129)(1882+129)$, where 1753 and 2011 are non-trivial factors of n

(b) It $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv \pm y \pmod{n}$, then $n \mid (x^2 - y^2) = (x-y)(x+y)$, but n does not divide any of the two factors. It is enough to show that $\gcd(n, x+y) \neq 1$. If it was so, then $1 = an + b(x+y)$ for some a, $b \in \mathbb{Z}$, and so

$$x - y = an(x-y) + b(x-y)(x+y)\,.$$

But n divides both summands on the right, hence also the LHS. But this contradistcs the fact that n does not divide $x - y$.

(c) For $n = 642401$, we are given

$$516107^2 \equiv 7 \pmod{n}\,,$$

and

$$187722^2 \equiv 2^2 \cdot 7 \pmod{n}\,.$$

We try to find a factor of n "by hand".
Multiplying the first equation by 2^2 and subtracting the second one gives

$$2^2 \cdot 516107^2 - 187722^2 \equiv 0 \pmod{n}\,.$$

So we find that

$$(2 \cdot 516107 - 187722)(2 \cdot 516107 + 187722)$$

is divisible by n, and hence we can try to use, as in part (b), the gcd of $2 \cdot 516107 + 187722 = 1032214 + 187722 = 1219936$ and n, which is obtained by the Euclidean algorithm as

$$\begin{aligned}
1219936 &= 642401 + 577535\\
642401 &= 577535 + 64866\\
577535 &= 8 \cdot 64866 + 58607\\
64866 &= 58607 + 6259\\
58607 &= 9 \cdot 6259 + 2276\\
6259 &= 2 \cdot 2276 + 1707\\
2276 &= 1707 + 569
\end{aligned}$$

$$1707 = 3 \cdot 569\,.$$

Conclusion: one factor of n is 569, the other one being 1129, both being primes.

(7) (a) We get $m = d \cdot e - 1 = 11600000$ whose binary expansion is as given in the question. So $m/16 = 725000$ and, using the squaring method, we find $\rho = 3^{m/16} \equiv 34485 \pmod{n}$ (with $n = 93433$).

(b) Since $3^{m/16} \equiv 34485 \not\equiv 1 \pmod{n}$, and the fact that $\rho^2 \equiv 1 \pmod{93433}$, the algorithm in the lectures suggest that we should try $\gcd(\rho - 1, n) = \gcd(34484, 93433) = 233$, and we find

$$n = 93433 = 233 \cdot 401\,,$$

which is indeed a prime factorization.