MTH6115 **Cryptography**

Solutions 10

---

1 Factorise 1728 as $2^6.27$, and pick a value of x, say $x = 5$. Now we calculate $x^{27} \equiv 5^{27} \equiv 1217 \bmod 1729$, and keep squaring: $1217^2 \equiv 1065$, $1065^2 \equiv 1$. Since $1065 \neq \pm 1 \bmod 1729$ we have shown that 1729 is not prime.

Doing the same to 1753 yields $1752 = 2^3.219$ and $5^{219} \equiv 190 \bmod 1753$, and repeated squaring gives $190^2 \equiv 1040$, $1040^2 \equiv 1752 \equiv -1$. Try again with a random value of x, say $x = 1372$. We have $1372^{219} \equiv 1563 \bmod 1753$, and $1563^2 \equiv 1040 \bmod 1753$, which we already know squares to -1. It's already looking likely that 1753 is prime, but try a few more random values of x to increase our confidence. $285^{219} \equiv 190$, which we've already seen. $1117^{219} \equiv 713$ and $713^2 \equiv -1$, and so on. (In fact, 1753 is prime.)

2 We choose a value for b and try Pollard's method. If we don't succeed in finding a factor, we increase b and try again. For example, for $b = 4$, we get $2^{4!} \equiv 1256 \pmod{2573}$, and $\gcd(1255, 2573) = 1$, so we don't get a factor. Then, we increase to $b = 5$. We have $2^{5!} \equiv 280 \pmod{2573}$. We have $\gcd(279, 2573) = 31$, so 31 divides 2573. In fact, $2573 = 31 \cdot 83$.

3 First we need to calculate 46980^{521}. We have $521 = 2^9 + 2^3 + 1$.

i	0	1	2	3	4
$46980^{2^i} \pmod{137017}$	46980	50564	117893	29003	26646

i	5	6	7	8	9
$46980^{2^i} \pmod{137017}$	124239	90037	50564	117893	29003

So the encryption of $x = 46980$ is

$$y := x^{521} = 29003 \cdot 29003 \cdot 46980 \equiv 41768 \pmod{137017}$$

Now $de - 1 = 177660 = 2^2 \cdot 44415$. For a choice of a, we calculate modulo 137017 the values a^{44415}, $a^{2 \cdot 44415}$, $a^{4 \cdot 44415}$ (this last one should be 1), in the hope that some member of this sequence is 1 without the previous member being ± 1 modulo 137017. We find that $2^{2 \cdot 44415} \equiv -1 \pmod{137017}$ and that $3^{44415} \equiv$

$1 \pmod{137017}$, so that $a = 2$ and 3 are useless here. Clearly $a = 4$ is useless [why?]. Trying $a = 5$ works, for $5^{2 \cdot 44415} \equiv 16653 \pmod{137017}$ (and of course $5^{4 \cdot 44415} \equiv 1 \pmod{137017}$). We now obtain the factors of N via the calculations that $\gcd(16652, 137017) = 181$ and $\gcd(16654, 137017) = 757$. It is easily checked that $181 \cdot 757 = 137017$.

4 Since $p - 1$ is a factor of $e - 1$,we have $x^e \equiv x \pmod{p}$ for all x, and $x^{e-1} \equiv 1 \pmod{p}$ for all x with $p \nmid x$. We thus let $x = 2$, and calculate $y := x^{e-1} \pmod{N}$; we get $y = 149382248505$. We find that $\gcd(y - 1, N) = 505777$. The prime factorisation of N is $N = 505777 \cdot 817979$.

[How does one calculate $x^{e-1} \pmod{N}$ when x and e are such large numbers? You have to use the usual method: first write e in the binary form, then use the "squaring" table. You are allowed to use a simple calculator for this problem, but when x and e are not so large, you should not need that. Remember that you are not allowed to use a claculator on the exam.]

5 We have $de - 1 = 95472 = 2^4 \cdot 5967$, and $5967 = 2^{12} + 2^{10} + 2^9 + 2^8 + 2^6 + 2^3 + 2^2 + 2 + 1$. We have $2^{5967} \equiv 1 \pmod{7519}$, which is of no use to us, so let us try $x = 3$ in our algorithm. We get:

$$3^{5967} \equiv 3604 \pmod{7519},\ 3^{2 \cdot 5967} \equiv 3503 \pmod{7519} \text{ and } 3^{4 \cdot 5967} \equiv 1 \pmod{7519},$$

and calculating $\gcd(7519, 3502) = 103$ and $\gcd(7519, 3504) = 73$, gives us that $7519 = 73 \cdot 103$. Thus $\lambda(7519) = \mathrm{lcm}(72, 102) = 72.102/6 = 1224$. Using the Euclidean Algorithm to calculate $83^{-1} \pmod{1224}$ gives $d' = 59$.