MATC16 Cryptography and Coding Theory
Gábor Pete
University of Toronto Scarborough
gpete at utsc dot utoronto dot ca

Solutions for HW 3

Sorry, this problem set had more numeric computations than it should have had...

Problem 1. Let e, d be encryption and decryption exponents for RSA with modulus $n = pq$.

(a) Show that $m^p \equiv m \pmod{p}$ for any m (not necessarily relatively prime to p). You can assume Fermat's little theorem. **(1 pt)**

(b) Show that $m^{ed} \equiv m \pmod{n}$ for any m. Again, we've seen the case $\gcd(m, n) = 1$, so you may assume that $\gcd \neq 1$. Hint: use the Chinese Remainder Theorem. **(3 pts)**

Solution. (a) If $\gcd(m, p) = 1$, then Fermat gives $m^{p-1} \equiv 1 \pmod{p}$, then multiply by m. If $\gcd(m, p) \neq 1$, then, since p is a prime, $p \,|\, m$, hence $m^p \equiv 0 \equiv m \pmod{p}$.

(b) By the CRT, we want to prove that $m^{ed} \equiv m$ both (mod p) and (mod q). By symmetry, we can focus on one of them. If $\gcd(m, p) = 1$, then, since $m^{p-1} \equiv 1 \pmod{p}$ and $k(p-1)(q-1) = ed - 1$ for some integer k, we have that $m^{ed-1} \equiv 1^{k(q-1)} \equiv 1 \pmod{p}$, and we are done. If $\gcd(m, p) \neq 1$, then $p \,|\, m$, hence, unless $ed \equiv 0 \pmod{p-1}$, we have $p \,|\, m^{ed}$, too. But $p - 1$ divides $ed - 1$, so it cannot divide ed, so it's OK.

Problem 2. Take the 4-digit number formed by the end of your student ID. Find a number with difference at most 4 from it that is not divisible by any of 2,3,5, call it n. Choose a random base b (make an attempt to make it really random in $\{2, 3, \ldots, n-2\}$, not just 2 or 3), and test the primality of n with **(a)** the Fermat prime test and **(b)** the Miller-Rabin test, both times using the same base b. **(2+2 pts)**

Solution. My 4-digit number is 6413. Not divisible by any of 2,3,5. A random base is 1454.

(a) We need to calculate $1454^{6412} \pmod{6413}$. To prepare for successive squaring, write the exponent in base 2, $6412 = 4096 + 2048 + 256 + 8 + 4$. Now, $1454^2 \equiv 4239$, $1454^4 \equiv 4239^2 \equiv -105$, $1454^8 \equiv (-105)^2 \equiv 4612$, $4612^2 \equiv 5036$, $5036^2 \equiv 4294$, $4294^2 \equiv 1061$, $1061^2 \equiv 3446$, $1454^{256} \equiv 4453$, $4453^2 \equiv 213$, $213^2 \equiv 478$, $1454^{2048} = 478^2 \equiv 4029$, $1454^{4096} \equiv 4029^2 \equiv 1538$, all (mod 6413). Therefore, $1454^{6412} \equiv 1538 \cdot 4029 \cdot 4453 \cdot 4612 \cdot (-105) \equiv 4294 \pmod{6413}$. This is not 1, hence 6413 is not a prime.

(b) $6412 = 2^2 \cdot 1603$, hence $k = 2$ and $m = 1603$. First step is $b_0 \equiv 1454^{1603} = 1454^{1024+512+64+2+1} \equiv 478 \cdot 213 \cdot 1061 \cdot 4239 \cdot 1454 \equiv 1196 \pmod{6413}$, then $b_1 \equiv b_0^2 \equiv 317 \pmod{6413}$. This is $\not\equiv -1 \pmod{6413}$, hence 6143 is not a prime, again.

Problem 3. Suppose you want to factor $n = 2288233$, and you discover that $880525^2 \equiv 2 \pmod{n}$, and $2057202^2 \equiv 3 \pmod{n}$, and $648581^2 \equiv 6 \pmod{n}$, and $668676^2 \equiv 77 \pmod{n}$. Use this information to factor n. **(2 pts)**

Solution. Multiply the first three equations together to get

$$(880525 \cdot 2057202 \cdot 648581)^2 \equiv 2 \cdot 3 \cdot 6 \pmod{2288233}$$
$$1567892^2 \equiv 6^2 \pmod{2288233}.$$

Therefore, $2288233 \mid (1567892-6)(1567892+6)$, hence let's compute $\gcd(1567892-6, 2288233)$ using the Euclidean algorithm. $2288233 = 1 \cdot 1567886 + 720347$, then $1567886 = 2 \cdot 720347 + 127192$, then $720347 = 5 \cdot 127192 + 84387$, then $127192 = 1 \cdot 84387 + 42805$, then $84387 = 1 \cdot 42805 + 41582$, then $42805 = 1 \cdot 41582 + 1223$, then $41582 = 34 \cdot 1223 + 0$, hence gcd$= 1223$. We get $2288233 = 1223 \cdot 1871$.

Problem 4. $\alpha = 2$ is a primitive root mod $p = 101$. Alice and Bob want to use ElGamal with these parameters.

(a) What are the largest a for Bob and k for Alice that are worth choosing? In other words, these exponents should be random elements of what set? **(1 pt)**

(b) Assume that $a = 24$ and $k = 69$. Choose a message $1 < m < 100$ for Alice to send, and encrypt it. Then check that Bob can decrypt the ciphertext correctly, without knowing k. **(2 pts)**

Solution. (a) Since $\alpha^{100} \equiv 1 = \alpha^0 \pmod{101}$, we have $\alpha^x \equiv \alpha^y \pmod{101}$ whenever $x \equiv y \pmod{100}$. Hence it is not worth choosing exponents larger than 100. In fact, 100 is not worth choosing, either, because from $\alpha^a \equiv 1 \pmod{101}$ one can immediately see that $a \equiv 100 \pmod{101}$, and similarly, 1 is also obviously not a good choice. So, usually the sources suggest $2 \leq a, k \leq 99$, but I also accept the answer "at most 100".

(b) By repeated squaring, get $\beta \equiv \alpha^a \equiv 2^{24} \equiv 5$ and $r \equiv \alpha^k \equiv 2^{69} \equiv 3 \pmod{101}$. Then $\beta^k \equiv 5^{69} \equiv 37 \pmod{101}$. Let's choose $m = 49$. Then $t \equiv \beta^k m \equiv 96 \pmod{101}$, hence the ciphertext is $(3, 96)$.

To decrypt, want $96 \cdot 3^{-24} \pmod{101}$. Since $3 \cdot 34 \equiv 1 \pmod{101}$, we need to calculate $96 \cdot 34^{24}$, which is 49 (mod 101), great.

Problem 5. Suppose you have discovered that $3^6 \equiv 44 \pmod{137}$ and $3^{10} \equiv 2 \pmod{137}$. Find a value of x with $0 \leq x \leq 135$ such that $3^x \equiv 11 \pmod{137}$. (**2 pts**)

Solution. $3^6 \cdot 3^{-20} \equiv 44 \cdot 4^{-1} \pmod{137}$, hence $3^{-14} \equiv 11 \pmod{137}$. The exponent can be reduced (mod 136), hence $x = 122$ is the solution.

Problem 6. Consider the function $h(x) = x^2 \pmod p$, where p is a "large" prime, $p = 8848607$. Show that h is not preimage-resistant even for typical values (for 1, 4, 9, 16, etc, it is obviously easy to find preimages), and that it is not weakly collision free, either. **(2 pts)**

Solution. Note that $p \equiv 3 \pmod 4$, hence the Proposition on page 86 (which we did on class) tells us how to find a preimage effectively (if there is one, but either y or $-y$ does have a preimage). It is not weakly collision free (second preimage resistant) because if $h(x) = y$, then $h(p - x) = y$, too.

Problem 7. What is the probability that, in a family of five, all birthdays are in different months?

(a) First assume that all twelve months have equal lengths. **(1 pt)**

(b) In reality, different months have different lengths. Do you think this increases or decreases or doesn't change the above probability? You don't need to give a proof, but do give some support to your guess. **(2 pt)**

(c) How big does a family have to be to make the above probability zero? **(1 pt)**

Solution. (a) The probability of no collision is

$$\left(1 - \frac{1}{12}\right)\left(1 - \frac{2}{12}\right)\left(1 - \frac{3}{12}\right)\left(1 - \frac{4}{12}\right) \approx 38.2\% \,.$$

(b) For unequal lengths, the probability of no collision is smaller. One way to reach this conjecture is to look at the extreme case of having one extremely long month (almost one year) and 11 tiny ones (one nanosecond each). Then, with huge probability, all family members are born in the long month, so the probability for no collision is tiny. And it would be very strange if the probability was not minimized by one of the extreme cases (either all equal, or one very long month), so the maximum non-collision probability should happen in the equal lengths case.

Note that even though collision in a longer month is more likely than in a shorter month, having more longer-than-average (31 day) months than shorter-than-average ones in reality is irrelevant, because one has to understand the net effect of longer and shorter months. For instance, in the above extreme example, there is only one long month and 11 short months, but still, the probability of collision is huge.

Another clue could come from looking at the collision probability only between two people. If the lengths (in days) are $a_1 + \cdots + a_{12} = 365$, then the probability of collision is $\sum_{i=1}^{12} (a_i/365)^2$. By the standard inequality between the arithmetic and quadratic means, this is minimized at $a_1 = \cdots = a_{12} = 365/12$. And it would be strange if the probability was changing in a different way for 2 than for 5 people.

The simplest analogue: for flipping coins, having no collision between two coins is maximized for fair coins, as easily computed.

(c) If all month lengths are positive, then there is still a positive probability of non-collision at 12 people, but zero at 13.