SECURITY

Assignment 8, Monday, November 27, 2017

S1013793 Carlo Jessurun
S1013792 Tony Lopar
Radboud University

Teaching assistant: Joost Rijneveld

Assignment 1

A. Given that we start on next friday, we would get
   Friday, November 24, 2017 + 1000 days = Thursday, August 20, 2020
B. In order to find the last digit we can take the mod10 of 2^{1893}, because the last digit is a number that's in the range of 0 to 9. In order to find the solution without calculator we may use Fermat's little theorem. Since 10 is not a prime, we should use the $a^p \equiv a \mod p$ part of the theorem.

   $2^{1893} \mod 10 = 2 \mod 1893 \mod 10$
   $= 2 \mod 10$
   $= 2$

Assignment 2

A. The multiplication table for $\mathbf{Z}_{10}$ is as follows:

$\mathbf{Z}_{10}$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	**3**	4	5	6	**7**	8	**9**
2	0	2	4	6	8	0	2	4	6	8
3	0	**3**	6	**9**	2	5	8	**1**	4	**7**
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	**7**	4	**1**	8	5	2	**9**	6	**3**
8	0	8	6	4	2	0	8	6	4	2
9	0	**9**	8	**7**	6	5	4	**3**	2	**1**

B. If we perform prime factorization of 10, we find that 10 = 2 * 5. This means that the elements where both multiplied numbers aren't a multiple of 2 or 5 have an inverse. These are 1, 3, 7 and 9. These numbers are made bold in the table of exercise A.

C. The numbers that aren't divisible by 3 or 5 don't have an inverse of mod 15. From the integers in $\mathbf{Z}_{15}$ these are: 0, 3, 5, 6, 9, 10, 12. We found these numbers by first perform a prime factorization on 15. This results in 15 = 3 * 5. A number x may only have an inverse of modulo 15 when gcd(x, 15) = 1. The prime factorization shown us that 15 consists of the primes 3 and 5. This means that multiples of 3 will have a gcd(x, 15) = 3 and multiples of 5 a gcd(x, 15) = 5. So these multiples don't have an inverse.

Assignment 3

Question	Solution
169 mod 11	**4**
−10 mod 6	**2**
175 mod 9	**4**
903−621 mod 9	282 mod 9 = **3**
175 · (903 − 621) mod 9	175 * (282) = 49350 = **3**

Assignment 4

Question	Solution
A. Find the factorization of 210	2 * 3 * 5 * 7
B. The prime factorization of 75 is $3^1 \cdot 5^2$. Find gcd(75, 210).	gcd(75, 210) = 3 * 5 = 15
C. Find the factorization of this greatest common divisor.	3 * 5
D. Factorize 198 and 135.	$2 * 3^2 * 11$ $3^3 * 5$
E. Give gcd(198, 135) in terms of all common prime divisors (2, 3, 5, and 11), i.e. use zero exponents in the product when a term is not present.	gcd(198, 135) = $2^0 * 3^2 * 5^0 * 11^0$
F. Now we generalize our findings in this last exercise. Let x = $p_1^{n1} \cdot ... \cdot p_k^{nk}$ and y = $p_1^{m1} \cdot ... \cdot p_k^{mk}$ be the factorizations of x and y, respectively, where prime factors p_i appear at least in one of the prime factorizations of x and y (thus, some of the exponents n_i or m_j may be 0). What is the factorization of gcd(x, y)?	The factorization of gcd(x, y) is a factorization with all p_i with the lower exponent of both. So, if x has 2^0 and y has 2^3, then we should take the 2^0 for the factorization.

Assignment 5

A. We can take x = 5 which gives
   $5 * 13 \equiv 1 \pmod{16}$
   $65 \equiv 1 \pmod{16}$

This holds, since 4 * 16 = 64 which shows that 65 gives a remainder of 1 on modulo 16.

B. In order to find out whether 12 has an inverse in Z_{170} we can compute gcd(12, 170) = 2. This means that 12 does not have an inverse, because the gcd(12, 170) ≠ 1 and therefore does not have an inverse.

Assignment 6

We cannot achieve perfect secrecy with a public-key cryptosystem. The reason for this is that the key will always compute the same ciphertext for the same plaintext where the ciphertext in one-time-pad differs every time. An attacker may try guess the plaintext by using the public key to encrypt the guess. After this, we can compare the ciphertext of the message with the ciphertext of the guess. If a part of the ciphertext matches, then we can derive that part of the plaintext from the ciphertext for future messages.