SECURITY

Assignment 9, Monday, December 4, 2017

S1013793 Carlo Jessurun
S1013792 Tony Lopar
Radboud University

Teaching assistant: Joost Rijneveld

Assignment 1

A. gcd(2145, 903) = 3. We can see this in the table below.

Pair	Remainder	Linear combination
(2145, 903)	339 = 2145 - 2 * 903	3 = 8 * 2145 - 19* 903 3 = 8 * (2145 - 2 * 903) - 3* 903
(903, 339)	225 = 903 - 2 * 339	3 = 8 * 339 - 3* 903 3 = 2 * 339 - 3* (903 - 2 * 339)
(339, 225)	114 = 339 - 1 * 225	3 = 2 * 339 - 3* 225 3 = 2 * (339 - 1 * 225) - 1* 225
(225, 114)	111 = 225 - 1* 114	3 = 2 * 114 - 1* 225 3 = 114 - 1 * (225 - 1* 114)
(114, 111)	3 = 114 - 1 * 111	3 = 114 - 1 * 111 3 = 0 * 111 + 1 * (114 - 1 * 111)
(111, 3)	0 = 111 - 37 * 3	3 = 0 * 111 + 1 * 3

B. No, since gcd(2145, 903) = 3 and to be relative prime the gcd of both values must be equal to 1.

C. gcd(1269, 137)

Pair	Remainder	Linear combination
(1269, 137)	36 = 1269 - 9 * 137	1 = -19 * 1269 + 176 * 137 1 = 5 * 137 - 19 * (1269 - 9 * 137)
(137, 36)	29 = 137 - 3 * 36	1 = 5 * 137 - 19 * 36 1 = 5 * (137 - 3 * 36) - 4 * 36
(36, 29)	7 = 36 - 1 * 29	1 = 5 * 29 - 4 * 36 1 = 29 - 4 * (36 - 1 * 29)
(29, 7)	1 = 29 - 4 * 7	1 = 29 - 4 * 7 1 = 0 * 7 + 1 * (29 - 4 * 7)
(7, 1)	0 = 7 - 7 * 1	1 = 0 * 7 + 1 * 1

D. 1269 and 137 are relative prime since there gcd is 1.

E. In the table of exercise C we can see that we can take n = -19 and m = 176.

F. The inverse is 176. If we calculate 176 * 137 mod 1269 we see that this indeed is equivalent to 1.

Assignment 2

A. $\mathbf{Z}^*_{17}$ contains the numbers from 1 to 16.
   $\phi(17) = 16$ since 17 is already a prime integer.

B. $\mathbf{Z}^*_{21}$ contains the numbers from 1 to 20. In order to calculate $\phi(21)$ we first have to find which primes make 21. This are the primes 3 and 7.

$$\begin{aligned}\phi(21) &= \phi(3*7)\\ &= 3 * 7 -(3 -1)-(7 -1)-1\\ &= 3 * 7 - 3 - 7 +1\\ &= (3 -1)(7 - 1)\\ &= 2 * 6\\ &= 12\end{aligned}$$

C. 127 is a prime, so Euler's totient will be 127 - 1.
   $\phi(127) = 126$

D. $\phi(1651) = \phi(13 * 127)$

$$\begin{aligned}&= 13 * 127 -(13 -1)-(127 -1)-1\\ &= 13 * 127 - 13 - 127 +1\\ &= (13 -1)(127 - 1)\\ &= 12 * 126\\ &= 1512\end{aligned}$$

Assignment 3

In this exercise we calculated to modulo by multiplying the modulo values of the values of which the value exists. These values can be found in the second block of the answer and are put in an descending order of the exponent.

7^{1024}	$= 7^{512} * 7^{512}$	$= ((3 \bmod 13) * (3 \bmod 13)) \bmod 13$	$= 9 \bmod 13$	$= 9$
7^{512}	$= 7^{256} * 7^{256}$	$= ((9 \bmod 13) * (9 \bmod 13)) \bmod 13$	$= 81 \bmod 13$	$= 3$
7^{256}	$= 7^{128} * 7^{128}$	$= ((3 \bmod 13) * (3 \bmod 13)) \bmod 13$	$= 9 \bmod 13$	$= 9$
7^{128}	$= 7^{64} * 7^{64}$	$= ((9 \bmod 13) * (9 \bmod 13)) \bmod 13$	$= 81 \bmod 13$	$= 3$
7^{64}	$= 7^{32} * 7^{32}$	$= ((3 \bmod 13) * (3 \bmod 13)) \bmod 13$	$= 9 \bmod 13$	$= 9$
7^{32}	$= 7^{16} * 7^{16}$	$= ((9 \bmod 13) * (9 \bmod 13)) \bmod 13$	$= 81 \bmod 13$	$= 3$
7^{16}	$= 7^{8} * 7^{8}$	$= ((3 \bmod 13) * (3 \bmod 13)) \bmod 13$	$= 9 \bmod 13$	$= 9$
7^{8}	$= 7^{4} * 7^{4}$	$= ((9 \bmod 13) * (9 \bmod 13)) \bmod 13$	$= 81 \bmod 13$	$= 3$
7^{4}	$= 7^{2} * 7^{2}$	$= ((10 \bmod 13) * (10 \bmod 13)) \bmod 13$	$= 100 \bmod 13$	$= 9$
7^{3}	$= 7^{2} * 7$	$= ((10 \bmod 13) * (7 \bmod 13)) \bmod 13$	$= 70 \bmod 13$	$= 5$
7^{2}	$= 7 * 7$	$= 10 \bmod 13$		$= 10$
7^{1}	$= 7 * 1$	$= 7 \bmod 13$		$= 7$

$7^{2015} \bmod 13 = 7^{1024} * 7^{512} * 7^{256} * 7^{128} * 7^{64} * 7^{16} * 7^{8} * 7^{4} * 7^{3}$

$= (9 * 3 * 9 * 3 * 9 * 9 * 3 * 9 * 5) \bmod 13$

$= ((3^3 \bmod 13)(5 \bmod 13)(9^5 \bmod 13)) \bmod 13$

$= ((27 \bmod 13)(5 \bmod 13)((9^2 \bmod 13)(9^3 \bmod 13)) \bmod 13) \bmod 13$

$= (1 * 5 * ((81 \bmod 13)(729 \bmod 13)) \bmod 13) \bmod 13$

$= (5 * (3 * 1) \bmod 13) \bmod 13$

$= (5 * 3) \bmod 13$

$= (15) \bmod 13$

$= \mathbf{2}$

Assignment 4

A. The encryption with m = 14 will be as follows:

$\{m\}_{PK}$ $= 14^5 \bmod 299$

$= ((14^2 \bmod 299)(14^3 \bmod 299)) \bmod 299$

$= (196 \bmod 299)(2744 \bmod 299) \bmod 299$

$= (196 * 53) \bmod 299$

$= 10388 \bmod 299$

$= 222$

B. The prime factorization of this 299 is 13 * 23

$\phi(299) = \phi(13 * 23)$

$= 13 * 23 - (13 - 1) - (23 - 1) - 1$

$= 13 * 23 - 13 - 23 + 1$

$= (13 - 1)(23 - 1)$

$= 12 * 22$

$= 264$

C. We already know that e = 5 and $\phi(299) = 264$. The RSA private exponent is given by $d = e^{-1} \bmod (p - 1)(q - 1)$. This means that in order to find the exponent we need to find the inverse of n. Therefore we may use the extended Euclidean algorithm with the pair (299, 264).

Pair	Remainder	Linear combination
(299, 264)	35 = 299 - 1 * 264	1 = 83 * 299 - 94 * 264 1 = 83 * (299 - 1 * 264) - 11 * 264
(264, 35)	19 = 264 - 7 * 35	1 = 83 * 35 - 11 * 264 1 = 6 * 35 - 11 * (264 - 7 * 35)
(35, 19)	16 = 35 - 1 * 19	1 = 6 * 35 - 11 * 19 1 = 6 * (35 - 1 * 19) - 5 * 19
(19, 16)	3 = 19 - 1 * 16	1 = 6 * 16 - 5 * 19 1 = 1 * 16 - 5 * (19 - 1 * 16)
(16, 3)	1 = 16 - 5 * 3	1 = 1 * 16 - 5 * 3 1 = 0 * 3 + 1 * (16 - 5 * 3)
(3, 1)	0 = 3 - 3 * 1	1 = 0 * 3 + 1 * 1

From these computations we can see that the inverse is 94. So we may compute the exponent as follows:

d $= 94 \bmod 264$

$= 94$

This means that the secret key of Alice is defined by (299, 94).

D. First we will compute the ciphertext

c $= 3^5 \bmod 299$

$= 243 \bmod 299$

$= 243$

If you use a small exponent (IE 3) and you do not use any padding for encryption and you encrypt the exact same message with several distinct public keys, then your message is at

risk: if e = 3, and you encrypt message m with public keys n1, n2 and n3, then you have ci = m3 mod ni for i = 1 to 3. By the Chinese Remainder Theorem, you can then rebuild m3 mod n1,n2,n3, which turns out to be m3 (without any modulo) because n1n2n3 is a greater integer. A (non modular) cube root extraction then suffices to extract m.

Assignment 5

A. So when n = p * q holds we have the following case:

$\varphi(n) = \varphi(p * q)$
$= \varphi(p) * \varphi(q)$
$= (p - 1)(q - 1)$
$= pq - q - p + 1$
$= n + 1 - p - q$
$= n + 1 - (p + q)$

B. $\varphi(n) = 1540$

$1540 = (p - 1)(q - 1)$
$= n - q - p + 1$
$n = p \cdot (n - \varphi + 1 - p)$
$p,q = p^2 - (n - \varphi + 1) \cdot p + n = 0$
$= \frac{A \pm \sqrt{A^2 - 4n}}{2}$ with $A = n - \varphi + 1$

If we now take for example n = 1633

We get the following equation:

$P,q = \frac{94 \pm \sqrt{94^2 - 6532}}{2}$
$= \frac{94 \pm \sqrt{8836 - 6532}}{2}$
$= \frac{94 \pm \sqrt{2304}}{2}$
$= \frac{94 \pm 48}{2}$
$p = \frac{94 + 48}{2} = 71$
$q = \frac{94 - 48}{2} = 23$