Daniel Frey

CS 4920-001

Assignment 5

4/9/18

**Problem 1: Primitive Roots**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *a­* | *a2* | *a­3* | *a4* | *a5* | *a­6* |
| 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 4 | 1 | 2 | 4 | 1 |
| 3 | 2 | 6 | 4 | 5 | 1 |
| 4 | 2 | 1 | 4 | 2 | 1 |
| 5 | 4 | 6 | 2 | 3 | 1 |
| 6 | 1 | 6 | 1 | 6 | 1 |

Primitive roots of 7: 3, 5

**Problem 2: Miller-Rabin**

1. If a = 1, then in step 3 of TEST(n), it will test ‘if 1q mod n = 1 then return(“inconclusive”)’. This will return ‘inconclusive.’ If a = n – 1, then in step 5 of TEST(n), where j = 0, it will test ‘if (n – 1)q mod n = n – 1 then return(“inconclusive”)’ met by inspection.
2. Since 2047 – 1 = 2046 = 2 × 1023, calculate 21023. 21023 mod 2047 = (211)93 mod 2047 = (2048)93 mod 2047 = 1, therefore 2047 is a strong pseudoprime for base 2.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| n | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 22^n (mod 2047) | 2 | 4 | 16 | 256 | 32 | 1024 | 512 | 128 | 8 | 64 | 2 |

**Problem 3: En/decryption using RSA**

1. *n* = 33; φ(*n*) = 20; *d* = 3; C = 26.
2. *n* = 55; φ(*n*) = 40; *d* = 27; C = 14.
3. *n* = 77; φ(*n*) = 60; *d* = 53; C = 57.
4. *n* = 143; φ(*n*) = 120; *d* = 11; C = 106.
5. *n* = 527; φ(*n*) = 480; *d* = 343; C = 128. For decryption:

128343 mod 527 = 128256 × 12864 × 12816 × 1284 × 1282 × 1281 mod 527

= 35 × 256 × 35 × 101 × 47 × 128 = 2 mod 527

= 2 mod 257

**Problem 4: RSA Private Key**

By trial and error, *p* = 59 and *q* = 61. So φ(*n*) = 58 × 60 = 3480.

By extended Euclidean algorithm, the multiplicative inverse of 31 modulo φ(*n*) is 3031.

**Problem 5: Fast Exponentiation Algorithm**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *i* | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| *bi* | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| *c* | 1 | 2 | 4 | 5 | 11 | 23 | 46 | 93 | 186 | 372 |
| *f* | 5 | 25 | 625 | 937 | 595 | 569 | 453 | 591 | 59 | 1013 |