Cryptography
Homework #3 Solutions
Fall 2018

(1) For this problem you will be using RSA encryption with $\boldsymbol{n = 11522869,\ e = 717409}$

(a) Start with the message
NEVERTRUSTACOMPUTERYOUCAN'TTHROWOUTAWINDOW

Convert this into a number using ASCII code. You want to encode this, but the number is larger than $n$ (which is 8 digits). Break up the number into blocks of 7 digits. Now encode each block using RSA.

(b) Decode the message and convert back to characters.

First note that
$\boldsymbol{n = 11522869 = 2251 * 5119}$
$\boldsymbol{p = 2251,\ q = 5119}$

(a) Here is the message turned into ASCII
```
[78, 69, 86, 69, 82, 84, 82, 85, 83, 84, 65, 67, 79, 77, 80, 85, 84, 69, 82,
89, 79, 85, 67, 65, 78, 39, 84, 84, 72, 82, 79, 87, 79, 85, 84, 65, 87, 73,
78, 68, 79, 87]
```

Here is the message turned into blocks of 7 digits
```
[7869866, 9828482, 8583846, 5677977, 8085846, 9828979, 8567657, 8398484,
7282798, 7798584, 6587737, 8687987]
```

For each block compute the RSA encryption $x^e \pmod{n}$. We obtain the following list of encrypted blocks.
```
[8275545, 5748802, 3357001, 671906, 8718112, 10703352, 6768640, 3421209,
990630, 4058697, 8989855, 9361036]
```

(b) The inverse to $e$ is $\boldsymbol{d = e^{-1} \pmod{(p-1)(q-1)} = 6865489}$

For each encrypted block compute the RSA decryption $c^d \pmod{n}$. We obtain the following list of decrypted blocks.
```
[7869866, 9828482, 8583846, 5677977, 8085846, 9828979, 8567657, 8398484,
7282798, 7798584, 6587737, 8687987]
```

If we break this back up into blocks of two digits we get, as before:
```
[78, 69, 86, 69, 82, 84, 82, 85, 83, 84, 65, 67, 79, 77, 80, 85, 84, 69, 82,
89, 79, 85, 67, 65, 78, 39, 84, 84, 72, 82, 79, 87, 79, 85, 84, 65, 87, 73,
78, 68, 79, 87]
```

This converts back to the original message:
NEVERTRUSTACOMPUTERYOUCAN'TTHROWOUTAWINDOW

(2) Use RSA with public key $n = 1889570071$. To guard against transmission errors Alice has Bob encodes his message twice, with different values of the encryption exponent: $e_1 = 1021763679,\ e_2 = 519424709$. Eve intercepts the two coded messages $c_1 = 1244183534,\ c_2 = 732959706$. Assume Eve knows all of the numbers $n, e_1, e_2, c_1, c_2$. Determine the original message that Bob used.

First compute $\gcd(e_1, e_2) = 1$. Then compute $u, v$ such that $ue_1 + ve_2 = 1$. We compute these as $u = 252426389,\ v = -496549570$

Then in general $c_1^u c_2^v \equiv m^{\gcd(e_1,e_2)}\ (\text{mod}\, n)$. So in our example:

$$c_1^u c_2^v \equiv 1054592380 \equiv m^{\gcd(e_1,e_2)} \equiv m \quad (\text{mod}\, n) \Rightarrow m = 1054592380$$

(3) Use the Miller-Rabin test for the following numbers. If you find 10 numbers that are not Miller-Rabin witnesses then conclude that the number is probably prime.

(a) $n = 104513$

(b) $n = 406513$

(a) $n = 104513 \Rightarrow n - 1 = 104512 = 2^6 * 1633 \Rightarrow k = 6,\ q = 1633$

Try $a = 2$ as a possible Miller-Rabin witness.

$2^q \equiv 58750 \not\equiv 1\ (\text{mod}\, n)$

$2^q \not\equiv -1,\ 2^{2q} \equiv 20675,\ 2^{2^2 * q} \equiv 101968,\ 2^{2^3 * q} \equiv 101732,\ 2^{2^4 * q} \equiv 104512,\ 2^{2^5 * q} \equiv 1\ (\text{mod}\, n)$

Since none of the congruences on line 2 are -1, 2 is a witness for *n*. Hence *n* is **composite**.

(b) $n = 406513 \Rightarrow n - 1 = 2^4 * 25407 \Rightarrow k = 4,\ q = 25407$

Note for numbers that fail to be a witness we will only show the congruence that fails.

$a = 2$ fails because $2^{2^2 * q} \equiv -1\ (\text{mod}\, n)$

$a = 3$ fails because $3^{2 * q} \equiv -1\ (\text{mod}\, n)$

$a = 5$ fails because $5^{2^3 * q} \equiv -1\ (\text{mod}\, n)$

$a = 7$ fails because $7^{2^2 * q} \equiv -1\ (\text{mod}\, n)$

$a = 11$ fails because $11^{2^3 * q} \equiv -1\ (\text{mod}\, n)$

$a = 13$ fails because $13^{q} \equiv 1\ (\text{mod}\, n)$

$a = 17$ fails because $17^{q} \equiv -1\ (\text{mod}\, n)$

$a = 19$ fails because $19^{2^3 * q} \equiv -1\ (\text{mod}\, n)$

$a = 23$ fails because $23^{2^3 * q} \equiv -1\ (\text{mod}\, n)$

$a = 29$ fails because $29^{2^2 * q} \equiv -1\ (\text{mod}\, n)$

Since 10 possible witnesses failed we conclude that 406513 is probably prime (in fact it is prime).

(4) Use Pollard's $p-1$ method to factor each of the following.
(a) 1927
(b) 220459

(a) $n = 1927$. Try $a = 2$

$2^{2!} - 1 \equiv 3 \pmod{n}, \quad \gcd(3, n) = 1$

$2^{3!} - 1 \equiv 63 \pmod{n}, \gcd(63, n) = 1$

$2^{4!} - 1 \equiv 753 \pmod{n}, \gcd(753, n) = 1$

$2^{5!} - 1 \equiv 1394 \pmod{n}, \gcd(1394, n) = 41, n/41 = 47$

$n = 41 * 47$

(b) $n = 220459$. Try $a = 2$

$2^{5!} - 1 \equiv 85053 \pmod{n}, \quad \gcd(85053, n) = 1$

$2^{6!} - 1 \equiv 4045 \pmod{n}, \quad \gcd(4045, n) = 1$

$2^{7!} - 1 \equiv 43102 \pmod{n}, \gcd(43102, n) = 1$

$2^{8!} - 1 \equiv 179600 \pmod{n}, \gcd(179600, n) = 449, \quad n/449 = 491$

$n = 449 * 491$

(5) Samantha uses a RSA signature with primes $p = 541, q = 1223$ and public verification exponent $e = 159853$.
(a) Find Samantha's public modulus and private signing key.
(b) For the digital document $D = 630579$ what is Samantha's signature?

(a) $n = pq = 661643, d \equiv e^{-1} \pmod{((p-1)(q-1))} \equiv 159853^{-1} \pmod{659880} \equiv 561517 \pmod{659880}$

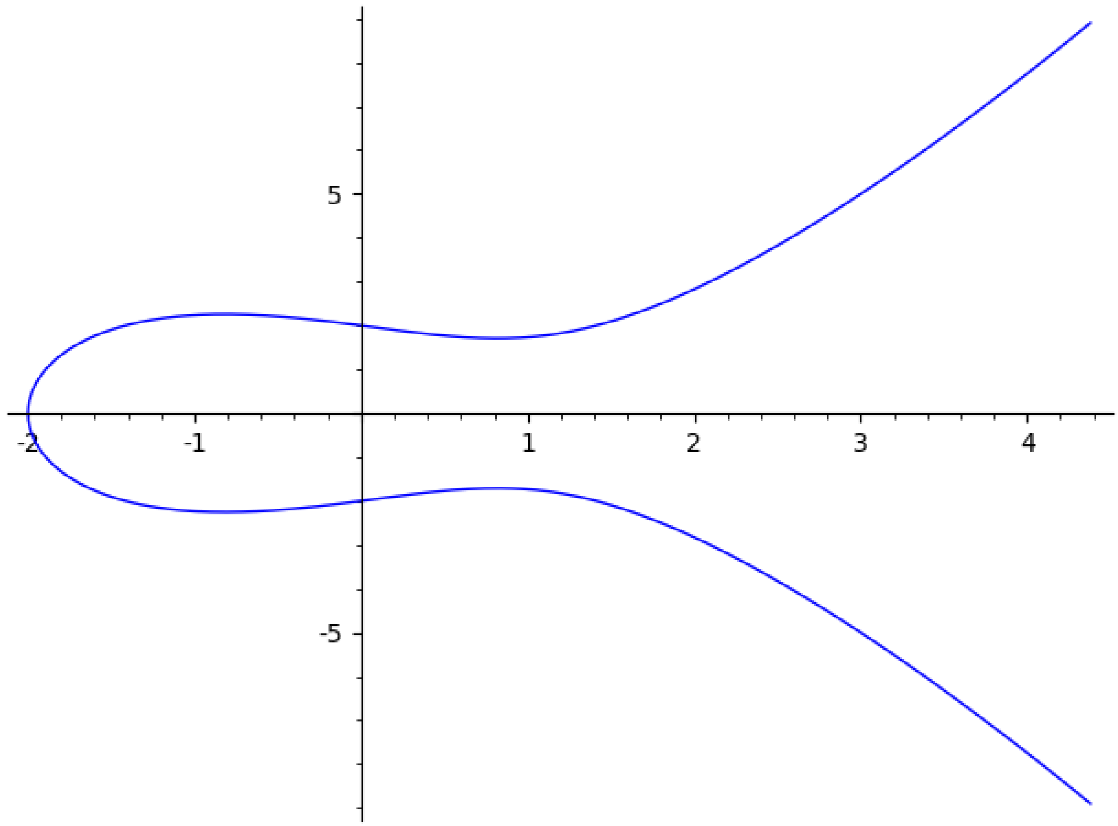
(b) $S \equiv D^d \pmod{n} \equiv 206484 \pmod{n}$ (note $S^e \equiv 206484^{159853} \equiv 630579 \pmod{n} = D$ )

(6) Prove that 1105 is a Carmichael number.

$1105 = 5 * 13 * 17$ Let $a$ be relatively prime to 1105. We then have
By Fermat's Little Theorem, $a^4 \equiv 1 \pmod{5}, a^{12} \equiv 1 \pmod{13}, a^{16} \equiv 1 \pmod{17}$
Hence $a^{48} \equiv 1 \pmod{1105} \Rightarrow a^{1104} \equiv 1 \pmod{1105}$. This proves that 1105 is a Carmichael number.

(7) For the elliptic curve $y^2 = x^3 - 2x + 4$
(a) Sketch the graph of the curve.
(b) Compute the following points: $P+Q, P-Q, 2P, 2Q, 3P$ for $P = (0,2), Q = (3,-5)$
(c) Display these points on your graph.

(a)




(b)

$\boldsymbol{P+Q=(22/9,\ 100/27)}$

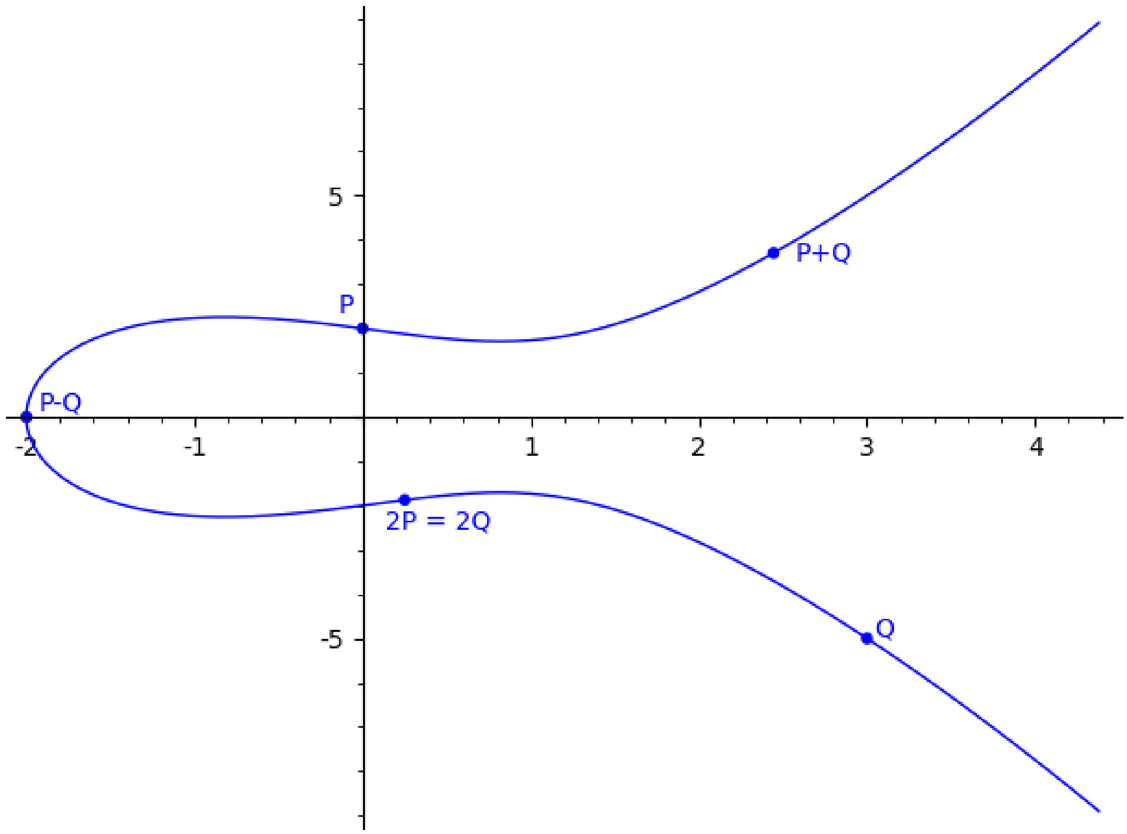
$\boldsymbol{P-Q=(-2,\ 0)}$

$\boldsymbol{2P=(1/4,\ -15/8)}$

$\boldsymbol{2Q=(1/4,\ -15/8)}$

$\boldsymbol{3P=(240,\ 3718)}$

(c) Note 3P is not displayed because it is outside of the plot area of the graph.




(8) For the elliptic curve $y^2 = x^3 + 2x + 3$ over $\mathbb{F}_7$.
(a) How many points are on the curve?
(b) Write an addition table for the curve.

(a) The curve has 6 points: $E(\mathbb{F}_7) = \{0, (2,1), (2,6), (3,1), (3,6), (6,0)\}$

(b)

| | **0** | **(2,1)** | **(2,6)** | **(3,1)** | **(3,6)** | **(6,0)** |
|---|---|---|---|---|---|---|
| **0** | 0 | (2,1) | (2,6) | (3,1) | (3,6) | (6,0) |
| **(2,1)** | (2,1) | (3,6) | 0 | (2,6) | (6,0) | (3,1) |
| **(2,6)** | (2,6) | 0 | (3,1) | (6,0) | (2,1) | (3,6) |
| **(3,1)** | (3,1) | (2,6) | (6,0) | (3,6) | 0 | (2,1) |
| **(3,6)** | (3,6) | (6,0) | (2,1) | 0 | (3,1) | (2,6) |
| **(6,0)** | (6,0) | (3,1) | (3,6) | (2,1) | (2,6) | 0 |