CRYPTOGRAPHY
SAMPLE FINAL
FALL '18

(1) Suppose $\boldsymbol{n = 11*13,\ e_1 = 35,\ e_2 = 49}$.
(a) One of $\boldsymbol{e_1, e_2}$ is a valid RSA encryption key for RSA (with modulus *n*) and the other is not. Explain which is which and why.
(b) Use the valid key to find the decryption key *d*.
(c) Use this decryption key to decrypt the ciphertext $\boldsymbol{c = 12}$

(2) Use the Miller-Rabin test for the $\boldsymbol{n = 45}$. If you find 3 numbers that are not Miller-Rabin witnesses then conclude that the number is probably prime.

(3) Use Pollard's $p - 1$ method to factor 319.

(4) For the elliptic curve $\boldsymbol{E : y^2 = x^3 + x + 1}$ over $\mathbb{F}_7$. Let $\boldsymbol{P = (2,5)}$
(a) Find the number of points on E.
(b) Compute $\boldsymbol{Q = P + P,\ P + Q,\ P - Q}$

(5) Use the double and add algorithm on the elliptic curve $\boldsymbol{y^2 = x^3 + x + 3}$ over $\mathbb{F}_7$ to compute $\boldsymbol{5P}$ for $\boldsymbol{P = (4,1)}$.

Solutions:

(1) (a) Note that $n = pq = 11*13 = 143, (p-1)*(q-1) = 120$. $e_1 = 35$ and 120 are not relatively prime (they have a common factor of 5). But $e_2 = 49$ and 120 are relatively prime. Therefore 49 is a valid encryption key but 35 is not.

(b) To find $d \equiv 49^{-1} \pmod{120}$ use the extended Euclidean algorithm.

$$\begin{aligned}
120 &= 2*49+22\\
49 &= 2*22+5\\
22 &= 4*5+2\\
5 &= 2*2+1
\end{aligned}$$

$$\begin{aligned}
1 &= 5-2*2\\
&= 5-2*(22-4*5) = 9*5-2*22\\
&= 9*(49-2*22)-2*22 = 9*49-20*22\\
&= 9*49-20*(120-2*49)\\
&= 49*49-20*20
\end{aligned}$$

Hence $d \equiv 49 \pmod{120}$

(c)
$$\begin{aligned}
&m \equiv c^d \pmod{n} \equiv 12^{49} \pmod{143} \equiv 12^{32+16+1} \pmod{143}\\
&12 \equiv 12 \pmod{143}\\
&12^2 \equiv 144 \equiv 1 \pmod{143}\\
&m \equiv 12^{32}12^{16}12^1 \equiv 12 \pmod{143}
\end{aligned}$$

(2) First not that $n-1 = 44 = 2^2 * 11$. So in Miller-Rabin, $k = 2, q = 11$ Use $a = 2$.

$$\begin{aligned}
&a^q = 2^{11} \equiv 2^{8+2+1} \pmod{45}\\
&(2 \equiv 2,\ 2^2 \equiv 4,\ 2^4 \equiv 16,\ 2^8 \equiv 16^2 \equiv 256 \equiv 31 \pmod{45})\\
&2^{11} \equiv 31*4*2 \equiv 23 \not\equiv 1 \pmod{45}\\
&2^{11} \not\equiv -1 \pmod{45}\\
&a^{2q} \equiv 2^{22} \equiv 2^{16+4+2} \pmod{45}\\
&(2^{16} \equiv 31^2 \equiv 16 \pmod{45})\\
&2^{22} \equiv 16*16*4 \equiv 34 \not\equiv -1 \pmod{45}
\end{aligned}$$

Therefore 2 is a Miller-Rabin witness and 45 is not prime.

(3)

$$2^{2!} \equiv 4 \text{ (mod 319)},\ \gcd(3,319)=1$$
$$2^{3!} \equiv 2^{6} \equiv 64 \text{ (mod 319)},\ \gcd(63,319)=1$$
$$2^{4!} \equiv 2^{24} \equiv 49 \text{ (mod 319)},\ \gcd(48,319)=1$$
$$2^{5!} \equiv 2^{120} \equiv 111 \text{ (mod 319)},\ \gcd(110,319)=11$$
$$p=11,\ q=n/11=29$$

(4) (a) The possible values of x: 0,1,2,3,4,5,6

$$x=0,\ y^2=x^3+x+1=1 \Rightarrow y=\pm 1 \text{ (mod 7)} \Rightarrow y=1,\ 6 \Rightarrow \text{Points } (0,1),\ (0,6)$$
$$x=1,\ y^2=x^3+x+1=3,\ \text{No points}$$
$$x=2,\ y^2=x^3+x+1=11 \equiv 4 \text{ (mod 7)} \Rightarrow y=\pm 2 \text{ (mod 7)} \Rightarrow y=2,\ y=5 \Rightarrow \text{Points } (2,2),(2,5)$$
$$x=3,\ y^2=x^3+x+1=31 \equiv 3 \text{ (mod 7)},\ \text{No points}$$
$$x=4,\ y^2=x^3+x+1=69 \equiv 6 \text{ (mod 7)},\ \text{No points}$$
$$x=5,\ y^2=x^3+x+1=131 \equiv 5 \text{ (mod 7)},\ \text{No points}$$
$$x=6,\ y^2=x^3+x+1=223 \equiv 6 \text{ (mod 7)},\ \text{No points}$$

There are 5 points on $E(\mathbb{F}_7)=\{O,\ (0,1),\ (0,6),\ (2,2),\ (2,5)\}$.

(b)

$$P+P$$
$$(x_1,y_1)=(2,5),\ (x_2,y_2)=(2,5)$$
$$\lambda=\frac{3x_1^2+A}{2y_1} \text{ (mod 7)}=2$$
$$x_3=\lambda^2-x_1-x_2=0,\ \ y_3=\lambda(x_1-x_3)-y_1=6$$
$$Q=P+P=(0,6)$$
$$P+Q$$
$$(x_1,y_1)=(2,5),\ (x_2,y_2)=(0,6)$$
$$\lambda=\frac{y_2-y_1}{x_2-x_1} \text{ (mod 7)}=3$$
$$x_3=\lambda^2-x_1-x_2=0,\ \ y_3=\lambda(x_1-x_3)-y_1=1$$
$$P+Q=(0,1)$$

$$P-Q$$
$$(x_1,y_1)=(2,5),\ (x_2,y_2)=(0,-6)=(0,1)$$
$$\lambda=\frac{y_2-y_1}{x_2-x_1} \text{ (mod 7)}=2$$
$$x_3=\lambda^2-x_1-x_2=2,\ \ y_3=\lambda(x_1-x_3)-y_1=2$$
$$P-Q=(2,2)$$

(5) We use the formulas for adding points on an elliptic curve to compute the following table.

n	***Q***	***R***
5	(4,1)	0
2	(6,6)	(4,1)
1	(6,1)	(4,1)
0	0	(4,6)