CRYPTOGRAPHY
SAMPLE MID-TERM
FALL 2018

(1) Use the Extended Euclidean Algorithm to compute gcd(175, 315) and then write it as a linear combination of 175 and 315.

(2) Determine if *x* is invertible in $\mathbb{Z}_n$. If it is then find x^{-1}.

(a) $\boldsymbol{x = 16}$ in $\mathbb{Z}_{\mathbf{99}}$

(b) $\boldsymbol{x = 350}$ in $\mathbb{Z}_{\mathbf{441}}$

(3) (a) Use Euler's Product Formula to compute $\boldsymbol{\phi(36)}$. Check your answer by finding the elements of U(36).

(b) Use Euler's Product Formula to compute $\boldsymbol{\phi(1485)}$.

(4) (a) Use the Fast Power algorithm to compute $\mathbf{11^{70} \bmod 13}$. Hint, reduce the power as much as possible first.

(b) Use whatever method you want to compute $\mathbf{33^{577} \pmod{323}}$ (note 323 = 17*19).

(5) (a) Find the order of 11 in U(15).

(b) Determine whether or not 5 is a primitive root of U(17)

(c) Determine whether or not 5 is a primitive root of U(62).

(6) (a) Prove that if *a* and *b* are positive integers and $\boldsymbol{x^a \equiv 1 \pmod{n},\ x^b \equiv 1 \pmod{n}}$ then $\boldsymbol{x^{\gcd(a,b)} \equiv 1 \pmod{n}}$

(b) Use the result in (a) to solve $\boldsymbol{x^{10} \equiv 1 \pmod{2027}}$ (note 2027 is prime)

(7) Solve the following Chinese Remainder problem. Find the smallest positive solution and the general solution. $\boldsymbol{x \equiv 4 \pmod{3},\ x \equiv 3 \pmod{5},\ x \equiv 2 \pmod{8}}$

(8) Suppose that Eve is able to solve the Diffie-Hellman problem. That is, given that Eve knows $\boldsymbol{g^a}$ and $\boldsymbol{g^b}$ she is able to compute $\boldsymbol{g^{ab}}$ (these are all done mod *p* for some prime *p*). Show that Eve can break the Elgamal encryption scheme.

SOLUTIONS:

(1) gcd(175, 315)

$$\mathbf{315 = 175 + 140}$$
$$\mathbf{175 = 140 + 35}$$
$$\mathbf{140 = 4 * 35 + 0}$$
$$\mathbf{gcd(175, 315) = 35}$$

Write gcd as linear combination

$$\mathbf{35 = 175 - 140 = 175 - (315 - 175) = 2 * 175 - 315}$$

(2) (a)

$$\mathbf{99 = 6 * 16 + 3}$$
$$\mathbf{16 = 5 * 3 + 1 \Rightarrow gcd(16, 99) = 1}$$
$$\mathbf{1 = 16 - 5 * 3 = 16 - 5 * (99 - 6 * 16) = 31 * 16 - 5 * 99}$$
$$\mathbf{16^{-1} \equiv 31 \pmod{99}}$$

(b) Note that 350 and 441 are relatively prime. They have a factor of 7 in common. Hence 350 does not have an inverse in $\mathbb{Z}_{441}$.

(3) (a) $\mathbf{36 = 2^2 * 3^2 \Rightarrow \phi(36) = 36 * \left(1 - \frac{1}{2}\right) * \left(1 - \frac{1}{3}\right) = 12}$

$$\mathbf{U(36) = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}}$$

(b) $\mathbf{1485 = 3^3 * 5 * 11 \Rightarrow \phi(1485) = 1485 * \left(1 - \frac{1}{3}\right) * \left(1 - \frac{1}{5}\right) * \left(1 - \frac{1}{11}\right) = 720}$

(4) (a) Note that $\mathbf{\phi(13) = 12 \Rightarrow 70 \equiv 10 \pmod{12} \Rightarrow 11^{70} \equiv 11^{10} \equiv 11^2 * 11^8 \equiv 1 * 1^4 \equiv 1 \pmod{12}}$

(b)

$$\mathbf{323 = 17 * 19 \Rightarrow \phi(323) = 323 * \left(1 - \frac{1}{17}\right) * \left(1 - \frac{1}{19}\right) = 288}$$
$$\mathbf{33^{577} \equiv 33^{2*288+1} \equiv 33 \pmod{323}}$$

(5)

(a)

$\mathbf{\phi(15) = \phi(3) * \phi(5) = 2 * 4 = 8 \Rightarrow 11^8 \equiv 1 \pmod{15}}$, hence the order of 11 is a divisor of 8.

$\mathbf{11^2 \equiv 121 \equiv 1 \pmod{15}}$.

The order of 11 in U(15) is 2.

(b)
$\phi(17)=16$ and the order of 5 is a divisor of 16. We need to check if $5^8 \equiv 1 \pmod{17}$
$5^8 \equiv 16 \pmod{17}$

Since none of these came out 1, the order of 5 is 16 hence 5 is a primitive root of U(17).

(c) Note that 5 and 62 are relatively prime, hence 5 is in U(62).

$\phi(62)=\phi(2*31)=30=2*3*5$ and the order of 5 is a divisor of 30.
Check the following powers: $30/2=15,\ 30/3=10,\ 30/5=6$
$5^{30/2} \equiv 5^{15} \equiv 1 \pmod{62}$. Hence 5 is not a primitive root in U(62)

(6) (a) By the extended Euclidean algorithm, $\gcd(a,b)=ua+vb$. Hence
$x^{\gcd(a,b)} \equiv x^{ua+vb} \equiv x^{ua}x^{vb} \equiv (x^a)^u(x^b)^b \equiv 1^u1^v \equiv 1 \pmod{n}$

(b) First note that $\phi(2027)=2026=2*1013$ and $\gcd(2026,10)=2$. We already know that $x^{2026} \equiv 1 \pmod{2027}$ and we want to find x so that $x^{10} \equiv 1 \pmod{2027}$. By (a) that means such an x would satisfy $x^{\gcd(2026,10)} \equiv x^2 \equiv 1 \pmod{2027} \Rightarrow x \equiv \pm 1 \pmod{2027} \Rightarrow x=1,\ 2026$ and these are the only solutions.

(7) $x \equiv 4 \pmod 3),\ x \equiv 3 \pmod 5,\ x \equiv 2 \pmod 8$
From the first congruence: $x=4+3y$. Plug into the second congruence:

$4+3y \equiv 3 \pmod 5 \Rightarrow 3y \equiv -1 \equiv 4 \pmod 5$
$3^{-1} \bmod 5 = 2$
$2*3y \equiv 2*4 \pmod 5 \equiv 3 \pmod 5$
$y \equiv 3 \pmod 5 \Rightarrow x=4+3*3=13$

The general solution of the first two congruences is: $x=13+3*5z=13+15z$. Now plug into the third congruence.

$13+15z \equiv 2 \pmod 8$
$15z \equiv 7z \equiv -11 \equiv 5 \pmod 8$
$15^{-1} \equiv 7 \pmod 8$
$7*7z \equiv 7*5 \equiv 35 \equiv 3 \pmod 8$
$z \equiv 3 \pmod 8 \Rightarrow x=13+15*3=58$

The general solution for al three congruences is $x=58+3*5*8k=58+120k$

(8) Eve knows the public key $\boldsymbol{A = g^a}$. She also knows the cipher texts $\boldsymbol{c_1 = g^k}$, $\boldsymbol{c_2 = m * A^k}$. Since Eve knows both $\boldsymbol{g^a}$, $\boldsymbol{g^k}$ she can compute $\boldsymbol{g^{ak}}$. This implies that she can compute $\boldsymbol{x = (g^{ak})^{-1}}$.

But then she can compute $\boldsymbol{x * c_2 = m}$, which means Eve has broken Elgamal.