Introduction to Cryptography: Homework #4

Due on June 16, 2019 at 3:10pm

Professor Manuel

ShiHan Chan

Problem 1

Part One

Prove for any prime p, $\varphi(p^k) = p^k - p^{k-1}$, $\varphi(x)$ is count of invertible elements in set Z/xZ(not include 0), so it is equal to number of elements in set minus number of elements that are not invertible. So $\varphi(x)$ is equal to x-1 minus count of numbers that are not coprime with x. Since p is prime, number that are not coprime with p^k must have p as a factor. So $p, 2p, 3p...p * p...(p^{k-1} - 1) * p$, there are $p^{k-1} - 1$ elements not coprime with p^k, so $\varphi(p^k) = (p^k - 1) - (p^{k-1} - 1) = p^k - p^{k-1}$.

Part Two

By using Chinese Remainder thereom, there exists a ring isomorphism between Z/mnZ and Z/mZ x Z/nZ since m,n are coprime integers. $\varphi(mn)$ is number of invertible elements in Z/mnZ, $\varphi(m)$ is number of invertible elements in Z/mZ, $\varphi(n)$ is number of invertible elements in Z/nZ. Isomorphism indicates there is a bijection betweens two set, so the number of elements in two sets are same. So $\varphi(mn) = \varphi(m) * \varphi(n)$

Part Three

Suppose $n = p_1^{a_1} * p_2^{a_2} * p_3^{a_3} * ...p_k^{a_k}$, p1...pk are different prime integers and a1...ak are integers. Different prime integers are coprime to each other, so we can get:

$\varphi(n) = \varphi(p_1^{a_1}) * \varphi(p_2^{a_2}) * ..... * \varphi(p_k^{a_k})$

$\varphi(n) = (p_1^{a_1} - p_1^{a_1-1}) * (p_2^{a_2} - p_2^{a_2-1}) * .....(p_k^{a_k} - p_k^{a_k-1})$

$\varphi(n) = p_1^{a_1} * (1 - \frac{1}{p_1}) * p_2^{a_2} * (1 - \frac{1}{p_2}) * .....p_k^{a_k} * (1 - \frac{1}{p_k})$

$\varphi(n) = n * \prod_{p|n}(1 - \frac{1}{p})$

Part Four

$1000 = 2^3 * 5^3$, so $\varphi(1000) = 1000 * (1 - \frac{1}{2}) * (1 - \frac{1}{5}) = 400$, and since 7 and 1000 are coprime integers,

$7^{400} \equiv 1 \mod 1000$.

$7^{800} \equiv 1 \mod 1000$

$7^{803} \equiv 7^3 \mod 1000$

$7^{803} \equiv 343 \mod 1000$

The last three digits are 343.

Problem 2

1. 128 bits 1 is used as key for round 1.
2. $K(5) = K(1) \oplus K(4)$
3. Suppose X is 4 bits long, we know that $X \oplus 1111 = \overline{X}$.

And K(0),K(1),K(2),K(3)=1111.
So we can see:
$K(10) = K(6) \oplus K(9) = (K(2) \oplus K(5)) \oplus (K(5) \oplus K(8)) = K(2) \oplus K(8) = \overline{K(8)}$
$K(11) = K(7) \oplus K(10) = (K(3) \oplus K(6)) \oplus (K(6) \oplus K(9)) = K(3) \oplus K(9) = \overline{K(9)}$

Problem 3

1.
In ECB mode, each block is encrypted seperately with block E and key K with single plaintext input. So if one block is corrupted, only one plaintext will be encrypted incorrectly.
In CBC mode, each block is encrypted with block E and key K, and the input of block is xor between previous ciphertext and current plaintext. So if one block is corrupted (not the last block, the penult block), two plaintext will be encrypted incorrectly.
2.
If IV is increased by 1 each time, the attacker will know the exact value of IV after the reset and attacker can contruct any plaintext and xor with IV, then put the result into block cipher. So he can compare the plaintext and ciphertext efficiently since he knows the input of the block. So CPA is not secure.
3.
$p-1=28$, and 28 has prime factor q=2,7.
When q=2, $2^{\frac{p-1}{q}}=2^{14}\equiv 28 \mod 29$.
When q=7, $2^{\frac{p-1}{q}}=2^{4}\equiv 16 \mod 29$.
Since for all primes q=2,7 such that $q|(p-1)$, $2^{\frac{p-1}{q}}\not\equiv 1 \mod 29$, 2 is a generator of $U(Z/29Z)$.
4.
We can use second proposition on slide 157.
$(\frac{1801}{8191})\equiv 1801^{4095} \mod 8191$
Use modular exponention (calculator) to get following:
$1^2*1801\equiv 1801 \mod 8191$
$1801^2*1801\equiv 2493 \mod 8191$
$2493^2*1801\equiv 6873 \mod 8191$
$6873^2*1801\equiv 7874 \mod 8191$
$7874^2*1801\equiv 544 \mod 8191$
$544^2*1801\equiv 557 \mod 8191$
$557^2*1801\equiv 1193 \mod 8191$
$1193^2*1801\equiv 4482 \mod 8191$
$4482^2*1801\equiv 6085 \mod 8191$
$6085^2*1801\equiv 5027 \mod 8191$
$5027^2*1801\equiv 4046 \mod 8191$
$4046^2*1801\equiv 8190 \mod 8191$
So $(\frac{1801}{8191})\equiv 1801^{4095}\equiv -1 \mod 8191$
$(\frac{1801}{8191})=-1$
5.
If $b^2-4ac=0$, $(\frac{b^2-4ac}{p})=0$, the only solution is $x=\frac{-b}{2a} \mod p$, and the number of solution satisfies $1+(\frac{b^2-4ac}{p})=1+0=1$.
If $b^2-4ac\neq 0$, $(\frac{b^2-4ac}{p})\neq 0$, the two solutions are $x=\frac{-b\pm\sqrt{b^2-4ac}}{2a} \mod p$.And we can get:
$x\equiv \frac{-b\pm\sqrt{b^2-4ac}}{2a} \mod p$
$\pm(2ax+b)\equiv\sqrt{b^2-4ac} \mod p$
If $(\frac{b^2-4ac}{p})=1$, b^2-4ac is square mod p, and there are two solutions, the number of solution equals to $1+(\frac{b^2-4ac}{p})=1+1=2$.
If $(\frac{b^2-4ac}{p})=1$, b^2-4ac is not square mod p, and there are no solution, the number of solution equals to $1+(\frac{b^2-4ac}{p})=1-1=0$.
6.
Since gcd(n,pq)=1 implies gcd(n,p)=gcd(n,q)=1, p,q are both coprime with n and they are all primes, according to euler's thereom, $n^{p-1}\equiv 1 \mod p$, $n^{q-1}\equiv 1 \mod q$.

Problem 3 continued on next page...

q-1 divides p-1, suppose (q-1)*k=p-1, $(n^{q-1})^k = n^{p-1} \equiv 1 \mod q$, If gcd(n,pq)=1, according to chinese remainder thereom, $n^{p-1} \equiv 1 \mod pq$
7.
$\Leftarrow$: if p is an odd prime and $p \equiv 1 \mod 3$, $p \equiv 1 \mod 6$,then $-3 \not\equiv 0 \mod p$. $(\frac{-3}{p}) = (\frac{-1}{p}) * (\frac{3}{p})$, $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$
$\Rightarrow$:
8.
Since $(\frac{a}{p}) = 1$, assume $a \not\equiv 0 \mod p$, $(\frac{a}{p}) = a^{\frac{p-1}{2}} \equiv 1 \mod p$, 2 is a prime factor divides p-1, it doesn't satisfy for all prime factors q divides p-1, $a^{\frac{p-1}{q}} \not\equiv 1 \mod p$, so a is not a generator of F_p^*

Problem 4

1.
In integer domain (Z), suppose a prime integer p is reducible, so it can be expressed as p=ab (a,b are non-zero, non-invertible and $a, b \neq 1$). Let $x = t_1 a, y = t_2 b (t_1, t_2 \neq 0)$, and $x, y \neq 0$, if $b \not| t1$ and $a \not| t2, ab \not| t_1 a, ab \not| t_2 b$, which means $p \not| x, p \not| y$, and it's a contradiction with (*). So we prove that any prime element in integral domain, if it is reducible number then it is not prime.
2.
In integer domain(Z), suppose an irreducible number p¿1 is not prime, but irreducible number means that it cannot be expressed as p=ab ($a, b \neq 1$). Suppose a divides p, we can get a=1 or a=p, and it makes contraduction with (**). So we show that any irreducible integer is prime in Z.

3.
From (**), we know that any prime number is irreducible. If p is prime and p divides x*y ($x, y \in Z$), assume $p \not| x$ and $p \not| y$, we can get $p \not| xy$, and it's a contradiction. So (**) implies (*).
4.
We know any prime integer is irreducible from (*), if p is a prime and a divides p, assume $a \neq 1$ and $a \neq p$, then 1¡a¡p, but p is not reducible and it's a contradiction., so (*) implies (**). And we derive (**)implies (*) in previous part, we prove that (*) and (**) are equivalent in integer domain.

Problem 5

1 and 2.
Since 65337 is an odd prime, $(\frac{3}{65337}) = 3^{\frac{65337-1}{2}} \mod 65337$
We need to use modular exponention to claculate $3^{32768} \mod 65337$
We calculate $3^1, 3^2, 3^4 ..... 3^{256} ... 3^{32768}$ recursively (mult the exponention part by 2 each time)
$3 \equiv 3 \mod 65337$
$3^2 \equiv 9 \mod 65337$
$9^2 \equiv 81 \mod 65337$
.....(we done the calculation on calculator)
$65281^2 \equiv 65536 \mod 65537$
So $3^{32768} \equiv -1 \mod 65537$, and $3^{32768} \not\equiv 1 \mod 65537$
3.
3 is primitive root(generator) mod 65537. Since 2 is the only prime such that 2 divides (65537-1) (q divides p-1), and $3^{32768} \not\equiv 1 \mod 65537$, 3 is primitive root.