Quiz 4

11/9/2022 (Wednesday) in Class

Bring: Calculator

Bring: 1 sheet of typed or written notes front and back

Topics

Prime Factorization, Mod

Fermat's Theorem

Euler Phi Function

Euler's Theorem

Primality Testing (Miller-Rabin)

Discrete Log Problem

Factoring Methods (Fermat, Pollard-Rho)

Fast Modular Exponentiation

Diffee-Hellman Key Exchange

RSA Encryption

El Gamal Encryption

Sample Questions

1) (Determine the Prime Factorization of 158,059,200

$158,0592 \times 100 = 2^4 \times 2^2 \times 5^2 \times 98787$

$=2^4 \times 2^2 \times 5^2 \times 3 \times 32929$

$= 2^4 \times 2^2 \times 5^2 \times 3 \times 13 \times 2533$

$=2^4 \times 2^2 \times 5^2 \times 3 \times 13 \times 17 \times 149$

$= 2^6 \times 3 \times 5^2 \times 13 \times 17 \times 149$

Try dividing by each prime, first 11 works

2) Determine ϕ(158059200). Express your answer in prime factorized form.

$= \phi(2^6) \times \phi(3) \times \phi(5^2) \times \phi(13) \times \phi(17) \times \phi(149)$

$= (2^6 - 2^5)(3 - 1)(5^2 - 5)(13 - 1)(17 - 1)(149-1)$

$= 2^5 \times 2 \times 2^2 \times 5 \times 2^2 \times 3 \times 2^4 \times 2^2 \times 37$

$= 2^{16} \times 3 \times 5 \times 37$

3) Determine the remainder when 73^{1388} is divided by 199. Note that 199 is prime. For full

credit use Fermat's Theorem.

$73^{198} = 1 \bmod 199$

$73^{1388} = 73^{198x7 + 2} = (73^{198})^7 73^2 \equiv 1^7(5329) \equiv 155 \bmod 199$

4) Determine the remainder when 7^{7181} is divided by 2491. (Note: 2491 = 47 x 53.) For full

credit use Euler's Theorem.

Phi(47 x 53) = phi(47)xphi(53) = 46 x 52 = 2392

$7^{2392} = 1 \bmod 2491$

$7^{7181} = 7^{2392x3 + 5} = (7^{2392})^3 7^5 \equiv 1^3(16807) \equiv 1861 \bmod 2491$

5) (10 pts) Use the Fermat Factoring Method to factor 44,173. Please fill out the table below. Note:

More rows than necessary are provided.

X	**$x^2 - 44173$**	**is sq?**

211	**348**	**no**
212	**771**	**no**
213	**1196**	**no**
214	**1623**	**no**
215	**2052**	**no**
216	**2483**	**no**
217	**2916**	**yes (54)**

(217 – 54) x (217 + 54) = 163 x 271

6) (8 pts) 7 is a generator/primitive root mod 17. There are a total of 8 generators mod 17. List

These generators can be listed the form 7^a mod 17, 7^b mod 17, 7c mod 17, 7d mod 17, 7e mod 17,

7

f mod 17, 7g mod 17, and 7h mod 17, where 0 < a < b < c < d < e < f < g < h < 17. List the values

of a, b, c, d, e, f, g and h in order.

7^2 not a generator because $(7^2)^8 = 7^{16} = 1$ mod 17

Values of a,b,c,d,e,f,g,h do NOT share any common factors with 17-1 = 16.

1,3,5,7,9,11,13,15

7) (9 pts) Consider doing a Diffie-Hellman Key Exchange with the public keys p = 37 and g = 5.

Let Alice choose a private key of a = 15 and Bob choose a private key of b = 24. Calculate

(a) The value that Alice sends to Bob.

(b) The value that Bob sends to Alice.

(c) The shared key that both Alice and Bob will calculate at the end.

(a) 5, 25, 125 mod 37 = 14, -4

$5^4 = -4 \bmod 37$… $5^{15} = (5^4)^3 5^3 = (-64)(14) = 10(14) = 140 = 29$

(b) $(5^{12})^2 = 10^2 = 100 = 26 \bmod 37$

C) $5^{15 \times 24} = 5^{360}$, we know that $5^{36} = 1 \bmod 37$

$(5^{36})^{10} = 1^{10} = 1$

8) (10 pts) In an RSA system, p = 17, q = 31 and e = 91. What is d? (Note: Full credit will only be

given to responses that appropriately use the Extended Euclidean Algorithm.)

phi(n) = (17 – 1)(31 – 1) = 16 x 30 = 480

d = 91^{-1} mod 480

480 = 5 x 91 + 25

91 = 3 x 25 + 16

25 = 1 x 16 + 9

16 = 1 x 9 + 7

9 = 1 x 7 + 2

7 = 3 x 2 + 1

7 - 3 x 2 = 1
7 - 3(9 - 7) = 1
4 x 7 - 3 x 9 = 1
4(16 - 9) - 3 x 9 = 1
4 x 16 - 7 x 9 = 1

$4 \times 16 - 7(25 - 16) = 1$

$11 \times 16 - 7 \times 25 = 1$

$11(91 - 3 \times 25) - 7 \times 25 = 1$

$11 \times 91 - 33 \times 25 - 7 \times 25 = 1$

$11 \times 91 - 40 \times 25 = 1$

$11 \times 91 - 40(480 - 5 \times 91) = 1$

$11 \times 91 - 40 \times 480 + 200 \times 91 = 1$

$211 \times 91 - 40 \times 480 = 1$

Taking this equation mod 480 we find: $211 \times 91 \equiv 1 \pmod{480}$ It follows that $d = 211$.

9) (12 pts) Let the public elements of an El Gamal Cryptosystem be $q = 41$, $\alpha = 12$. Let Alice's

private key $XA = 17$. Do the following:

1. Calculate Alice's Public Key.

2. Calculate the ciphertext (C1, C2) when Bob sends a message to Alice where $M = 6$ and his

randomly chosen value $k = 19$.

1. YA = 12^{17} mod 41

$12^1 = 12$

$12^2 = 144 – 123 = 21$ mod 41

$12^4 = 21^2 = 441 = 31$ mod 41

$12^8 = (-10)^2 = 100 = 18$ mod 41

$12^{16} = (18)^2 = 324 = 37$

$12^{17} = 12^{16} \times 12 = (37 \times 12) = -4 \times 12 = -48 = 34$ mod 41.

M = 6, k = 19

$34^{19} = (-7)^{19} = (-7)^9(-7)^9(-7) = (13)(13)(-7) = 5(-7) = -35 = 6$

K = 6

C1 = $12^{19} = 12^{17}12^2 = (34)(21) = 17$

C2 = 6 x6 = 36