Adam Gincel

Professor Engling

5/6/2015

*I pledge my honor that I have abided by the Stevens Honor System.*

Homework 9

13:

A: 9 (4 mod 13) mod 13 = (9 \* 4) mod 13 = 10

C: (4 mod 13) (9 mod 13) mod 13 = 13 mod 13 = 0

E: (4 mod 13)^2 (9 mod 13) ^2 mod 13 = 97 mod 13 = 6

26: 5 integers congruent to 4 mod 12

4 mod 12 = 4

16 mod 12 = 4

28 mod 12 = 4

40 mod 12 = 4

52 mod 12 = 4

64 mod 12 = 4

Section 4.2

22:

(112)3 +

(210)3

=

(1022)3

----

(112)3 \*

(210)3

=

(101220)3

B:

(02112)3 +

(12021)3

=

(21210)3

----

(02112)3 \*

(12021)3

=

(111020122)3

26: 11^644 mod 645

1: x = 1, power = 11^2 mod 645 = 121 mod 645 = 121

2: x = 1, power = 121^2 mod 645 = 14641 mod 645 = 451

3: x = 451, power = 451^2 mod 645 = 203401 mod 645 = 226

4: x = 451, power = 226^2 mod 645 = 51076 mod 645 = 121

5: x = 451, power = 121^2 mod 645 = 14641 mod 645 = 451

6: x = 451, power = 451^2 mod 645 = 203401 mod 645 = 226

7: x = 451, power = 226^2 mod 645 = 51076 mod 645 = 121

8: x = 54571 mod 645 = 391, power = 121^2 mod 645 = 14641 mod 645 = 451

9: x = 391, power = 451^2 mod 645 = 203401 mod 645 = 226

10: x = 391\*226 mod 645 = 88366 mod 645 = 1, power = 226^2 mod 645 = 51076 mod 645 = 121

X = 1; 11^644 mod 645 = 1

Section 4.4

1: 15 is inverse of 7 mod 26

Gcd(7, 26) = 1, so an inverse exists.

26 = 3 \* 7 + 5

7 = 1 \* 5 + 2

5 = 2 \* 2 + 1

1 = 1\* 5 – 2 \* 2

1 = 1 \* 5 – (2 \* (7 – 1\*5)) = 3\*5 – 2\*7

1 = 3(26 – (3 \* 7)) – 2\*7 = 3 \* 26 – 11 \* 7

-11 is in inverse of 7 mod 26

26 – 11 = 15

15 is also an inverse of 7 mod 26.

6b: 34 mod 89

89 = 2 \* 34 + 21

34 = 1 \* 21 + 13

21 = 1 \* 13 + 8

13 = 1\*8 + 5

8 = 1\*5 + 3

5 = 1\*3 +2

3 = 1\*2 + 1

1 = 1\*3 – 1\*2

1 = 1\*3 – 1(5 – 1\*3) = 2\*3 – 1\*5

1 = 2(8 – 1\*5) – 1\*5 = 2\*8 – 3\*5

1 = 2\*8 – 3(13 – 1\*8) = 5\*8 – 3\*13

1 = 5(21 – 1\*13) – 3\*13 = 5\*21 – 8\*13

1 = 5\*21 – 8(34 – 1\*21) = 13\*21 – 8\*34

1 = 13(89 – 2\*34) – 8\*34 = 13\*89 – 34\*34

-34 mod 89 is congruent to 34 mod 89

89 – 34 = 55

55 mod 89 is also congruent to 34 mod 89

12a: 55 is congruent to 34 mod 89.

34\* (55 \* 77) mod 89 is congruent to 77 mod 89, so 34 (4235) mod 89 is congruent to 77 mod 39, so x = 4235.

20: x ≡ 2 (mod 3), x ≡ 1 (mod 4), and x ≡ 3 (mod 5)

53 mod 3 = 2, 53 mod 4 = 1, 53 mod 5 = 3

X = 53

34: 23^1002 mod 41

Gcd(23, 41) = 1

23^(41 – 1) = 1 mod 41

23^1002 = 23^(250\*40 + 2) = (23^40)^250 \* 23^2 = 1^250 \* 529 = 529 mod 41 = 37

Section 4.6

1a: DO NOT PASS GO

(G R Q R W S D V V J R)

5a: CEBBOXNOB XYG

SURRENDER NOW

24: Encrypt ATTACK

n = 43\*59

e = 17

ATTACK = 0019 1900 0210

=

0019^17 mod 2537

1900^17 mod 2537

0210^17 mod 2537

26: 3185 2038 2460 2550

n = 53\*61

e = 17

d = 2753

3185^2753 mod 3233 = 1816 = SQ

2038^2753 mod 3233 = 2008 = UI

2460^2753 mod 3233 = 1717 = RR

2550^2753 mod 3233 = 0411 = EL

SQUIRREL

30: Diffie-Hellman to generate a shared key, p = 101, a = 2, Alice selects k1 = 7, Bob selects k2 = 9

First Alice raises a to their k so 2^7, then mods it with p = 101, so 2^7 mod 101 = 27. Bob does the same on his end, doing a^k2 mod p so 2^9 mod 101, getting 7. Alice and Bob exchange results. Alice receives 7, and calculates 7^k1 mod p so 7^7 mod 101 = 90. Bob receives 27 and calculates 27^k2 mod p so 27^9 mod 101 which also equals 90. 90 is now Bob and Alice’s shared key.