Solutions to Assignment 11

Barr 4.6: 1, 2.

1. (a) Following Example 4.6.1 (Page 307), we find that σ = 70.

   (b) Given $(\tilde{x}, \tilde{\sigma})$ = (54,89), Bob regards the pair to be likely to be authentic since $54^7 \bmod 91 = 89$.

2. (a) Alice's encrypted pair is (185,21).

   (b) The original plaintext and signature are: $\tilde{x}$ = 44, $\tilde{\sigma}$ = 86. This is a valid signature pair since $\tilde{\sigma}^{e_A} \bmod 91 = 86^7 \bmod 91 = 44$.

Barr 4.7: 1*, 3, 7*

1.

n	$n^2 \pmod{39}$	n	$n^2 \pmod{39}$	n	$n^2 \pmod{39}$
0	0	13	13	26	13
1	1	14	1	27	27
2	4	15	30	28	4
3	9	16	22	29	22
4	16	17	16	30	3
5	25	18	12	31	25
6	36	19	10	32	10
7	10	20	10	33	36
8	25	21	12	34	25
9	3	22	16	35	16
10	22	23	22	36	9
11	4	24	30	37	4
12	27	25	1	38	1

Thus,

(a) The solutions to $x^2 \equiv 1 \pmod{39}$ are 1, 14, 25 and 38.

(b) The solutions to $x^2 \equiv 4 \pmod{39}$ are 2, 11, 28 and 37.

(c) The solutions to $x^2 \equiv 12 \pmod{39}$ are 18 and 21.

3.

n	$n^2 \pmod{31}$	n	$n^2 \pmod{31}$	n	$n^2 \pmod{31}$
0	0	13	14	26	25
1	1	14	10	27	16
2	4	15	8	28	9
3	9	16	8	29	4
4	16	17	10	30	1
5	25	18	14		
6	5	19	20		
7	18	20	28		
8	2	21	7		
9	19	22	19		
10	7	23	2		
11	28	24	18		
12	20	25	5		

Thus,

The solutions to $x^2 \equiv 1 \pmod{31}$ are 1 and 30.

The solutions to $x^2 \equiv 2 \pmod{31}$ are 8 and 17.

The solutions to $x^2 \equiv 8 \pmod{31}$ are 15 and 16.

7. The password s in the Fiat-Shamir setup is selected in the range 1 to n–1. Recall that $n = p \bullet q$, where p and q are both large prime numbers. Note that n is published and v is sent during login – so both are easily obtainable. If the password s is not relatively prime to n, then the greatest common divisor (gcd) of v and n is p or q (one of the primes!). Once p and q have been found, it is easy to find s and the system breaks down.

K1. In the Fiat-Shamir method, it is important to chose a modulus n = $p \bullet q$ which is hard to factor because once the factorization is known, obtaining s = $\sqrt{v} \pmod{n}$ is easy to calculate. Similarly, using a large prime n does not work because s = $\sqrt{v} \pmod{n}$ is easily calculated if n is prime.

K2. Using modulus P = 10111 and base B = 12, find the dlog of:

(a) $2401 = 7^4$.

dlog(7) = 3640 $\Rightarrow 12^{3640} \equiv 7 \pmod{10111}$.

$\therefore 2401 = 7^4 \equiv (12^{3640})^4 = 12^{14560}$. Using Fermat's Little Theorem, we can reduce the exponent 14560 mod 10110 = 4450.

$\therefore$ dlog(7^4) = 4450.

(b) $1001 = 7 \bullet 11 \bullet 13$.

dlog(1001) = dlog($7 \bullet 11 \bullet 13$) = dlog(7) + dlog(11) + dlog(13)

= 3640 + 250 + 4478 = 8368.

$\therefore$ dlog(1001) = 8368.

(c) 10100.

$10100 \equiv -11 \pmod{10111}$.

dlog(-11) = dlog(11) + dlog(-1). We are given dlog(11), so all we have to do now is calculate x = dlog(-1).

Using the definition of dlogs, $12^x \equiv -1 \pmod{10111}$

$\Rightarrow 12^{2x} \equiv 1 \pmod{10111}$. Since 10111 is prime, using Fermat's Little Theorem we know $12^{10111-1} = 12^{10110} \equiv 1 \pmod{10111}$.

Thus, letting 2x = 10110, we get x = 5055.

Thus, dlog(-1) = 5055 $\Rightarrow$ dlog(10110) = dlog(-11) = dlog(11) + dlog(-1)

= 250 + 5055 = 5305.

(d) 9889.

$9889 \equiv 9889 + 10111 \pmod{10111} = 20000 \pmod{10111}$.

$20000 = 2^5 \bullet 5^4$.

$\therefore \operatorname{dlog}(20000) = \operatorname{dlog}(2^5) + \operatorname{dlog}(5^4)$.

$\operatorname{dlog}(2^5) \equiv 5 \bullet \operatorname{dlog}(2) \pmod{10110} = 5 \bullet 4918 \pmod{10110}$

$= 24090 \pmod{10110} \equiv 3870$.

$\operatorname{dlog}(5^4) \equiv 4 \bullet \operatorname{dlog}(5) \pmod{10110} = 4 \bullet 9226 \bmod(10110)$

$= 36904 \pmod{10110} = 6574$.

$\therefore \operatorname{dlog}(9889) = \operatorname{dlog}(20000) = \operatorname{dlog}(2^5) + \operatorname{dlog}(5^4) = 3870 + 6574 = 10444$.

Reducing 10444 mod(10110), we obtain $\operatorname{dlog}(9889) = 334$.