Diffie Hellman

Knapsack

Feistel

DES

primitive roots

quadratic residue

Vernam

baby step/giant step

(5) The following questions are all related to theorems used to make the RSA system work.

(a) Say that we know $2015^2 \equiv 62666^2 \pmod{266923}$. Factor 266923 and use this to calculate $\phi(266923)$.

value of $\phi(266923)$: 265720

$2015^2 - 62666^2 \equiv 0 \pmod{266923}$

$(2015 - 62666)(2015 + 62666)$

$(-60651)(64681)$

$266923 = 911 \cdot 293$

$\phi(266923) = 910 \cdot 292$

$\gcd(266923, 60651) = \gcd(24319, 60651)$

$\gcd(12013, 24319)$

$\gcd(293, 12013) = 293$

(b) The number 268711 factors as $= 379 \cdot 709$. Use this fact to calculate

$5^{267629} \pmod{268711}$.

$\phi(268711) = 378 \cdot 708$

value of $5^{267629} \pmod{268711}$: 3125 $= 267624$

$5^{267629} \equiv 5^{267624+5} \equiv 5^5 \pmod{268711}$

(c) A three letter word is encoded to a longer number by $\ell_1 \cdot 64^2 + \ell_2 \cdot 64 + \ell_3$ where ℓ_1, ℓ_2, ℓ_3 are the numbers corresponding to the first second and third letters of the word. The cyphertext is given by the number 100717 and the modulus used is 268711. The public key is 199937. The following information may (or may not) be useful in recovering the plaintext.

$$50042 \cdot 267624 - 132971 \cdot 100717 =$$
$$10361 \cdot 199937 - 20568 \cdot 100717 =$$
$$257 \cdot 199937 - 192 \cdot 267624 = 1$$
$$87915 \cdot 199937 - 65414 \cdot 268711 = 1)$$
$$55502 \cdot 100717 - 20803 \cdot 268711 = 1 .$$

$e \cdot d \equiv 1 \pmod{\phi(m)}$

k	$100717^k \pmod{268711}$
2	73839 ✓
4	51731 ·
8	3512 ✓
16	242149
32	173469 ✓
64	161337 ✓
128	130421
256	230941 ✓
512	254912 ✓
1024	165013 ✓
2048	267117
4096	122437 ✓
8192	238412
16384	112625 ✓
32768	156581
65536	149210 ✓
131072	111617
262144	106596

100717 ✓

$60537 \equiv 57 \pmod{64}$ ← ℓ_3

$\left\lfloor \frac{60537}{64} \right\rfloor \equiv 945 \equiv 49 \pmod{64}$

$\left\lfloor \frac{945}{64} \right\rfloor \equiv 14 \pmod{64}$

$\ell_1 \quad \frac{60537}{64^2} \approx 14.\text{a bit}$

$60537 - 14 \cdot 64^2 = 3193$

$\ell_2 = \frac{3193}{64} = 49.\text{a bit}$

$\ell_3 = 57 = 3193 - 49 \times 64$

You may also want to know that $100717 = 23 \cdot 29 \cdot 151$. ϕ

Private key: ~~87915~~ 257

Number representing plaintext: 60537 $= 100717^{87915} \pmod{268711}$

Plaintext word: _____

~~$87915 = 65536 + 22379 = 65536 + 16384 + 5945$~~

~~$1945 = 4096 + 1024 + 512 + 256 + 64 + 32 + 8 + 2 + 1$~~

$257 = 256 + 1$

$\text{Plaintext} \equiv 100717^{257} \equiv 100717 \cdot 100717^{256}$

$\equiv 100717 \cdot 230941$

$\equiv 23 \cdot 29 \cdot 151 \cdot 230941$

$\equiv 23 \cdot 29 \cdot 208372$

$\equiv 23 \cdot 131146$

$\equiv 60537$

14, 49, 57 = Emu

(3) Using the Knapsack encryption system with a public modulus of 137 and a public key of

$$55 - 1 - 29 - 113 - 116 - 123$$

the message $50, 17, 63, 107, 100, 121$ was sent. Given that the first number of the private key is 1, what was the message? The encoding for the letters is given on the previous page.

(4) The ElGamal system is used with modulus 79 and 39 as a primitive root. Bob publishes his public key as 33. You may use the table of powers of 3 (*mod* 79) below to complete the computation.

(a) What is Bob's secret key?

(b) Alice sends the message $(52, 17), (57, 14), (13, 74)$. What three letter words does this message represent? Use the encoding $A \to 0, B \to 1, C \to 2$, etc.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
3^k	1	3	9	27	2	6	18	54	4	12	36	29	8	24	72	58	16	48
k	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
3^k	65	37	32	17	51	74	64	34	23	69	49	68	46	59	19	57	13	39
k	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53
3^k	38	35	26	78	76	70	52	77	73	61	25	75	67	43	50	71	55	7
k	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71
3^k	21	63	31	14	42	47	62	28	5	15	45	56	10	30	11	33	20	60
k	72	73	74	75	76	77												
3^k	22	66	40	41	44	53												

(5) Find all of the solutions to the following equations. You may use the table of powers of 3 (*mod* 79) on the previous page to help you.

(a) $33x \equiv 10 \pmod{79}$ $\equiv 41$

(b) $10^{33} \equiv x \pmod{79}$ $\equiv 22$

(c) $x^{11} \equiv 33 \pmod{79}$ $\equiv 15$

(d) $x^{33} \equiv 10 \pmod{79}$ $\equiv 9, 49, 21$

(e) Show that the equation

$$x^4 + 14x^2 + 43 \equiv 0 \pmod{79}$$

has no solutions.

(6) The integer 4667875 factors into primes as $107 \cdot 349 \cdot 5^3$.

(a) Calculate $\phi(4667875)$

(b) Calculate

$$7^{3688888} \pmod{4667875}$$

$3^{69} \cdot 3^y \equiv 3^{66} \pmod{79}$ $\quad 69 + y \equiv 66 \pmod{78}$

$10^{33} \equiv (3^{66})^{33} \equiv 3^{2178}$ $\quad 33 \cdot 41 \equiv 10 \pmod{79}$

$(x^2+7)^2 \Rightarrow x^4 + 14x^2 + 49 \equiv 6 \pmod{79}$

$\left(\frac{6}{79}\right) \equiv 6^{\frac{79-1}{2}} \equiv 6^{39} \equiv (3^5)^{39} \equiv 3^{39} \equiv 78 \equiv -1$

$x^2 \equiv b \pmod{p}$ $\quad \left(\frac{b}{p}\right) = \begin{cases} 1 & \text{if there is a sln.} \\ -1 & \text{if not} \end{cases}$

$y \equiv 63 \pmod{78}$

$-y \equiv -9 \cdot 7 \pmod{78}$

$x^{11} \equiv (3^y)^{11} \equiv 33 \equiv 3^{69}$ $\quad 7 \cdot 11 y \equiv 69 \cdot 7 \pmod{78}$

$7 \cdot 11 \equiv -1 \pmod{78}$

$x^{33} \equiv 10 \pmod{79}$

$(3^y)^{33} \equiv 3^{66} \pmod{79}$

$3y - 6 = 78k$

$y - 2 = 26k$

$x = 9, 49, 21$

$3y \equiv 6 \pmod{78}$

$33y \equiv 66 \pmod{78}$

$y \equiv 2$. but there are other solutions.

$y \equiv 2 \pmod{26}$

$y \equiv 2, 28, 54 \pmod{78}$