AN EXAMPLE OF BREAKING DIFFIE-HELMAN USING BABY-STEP/GIANT-STEP

$109^{15} \equiv 91 \cdot 109^{-17 \cdot 16} \Longrightarrow 91 \equiv 109^{17 \cdot 16 + 15}$

(1) Alice and Bob choose to exchange a key using the Diffie-Hellman key exchange system with prime modulus 269 and primitive root 109. Bob sends to Alice the the public key 91 and Alice sends to Bob the public key 210. Use the following data to determine the private keys of Alice and Bob and the common key that they share. Note: you should also be able to use the last column of the table to compute the common key since every power of 109 will be equivalent to 109^n for some $n < 17^2$. Then $109^n \equiv 109^{r+17q} \equiv 109^r \cdot 109^{17q}$ $(mod\ 269)$ for some r and q.

k	109^k $(mod\ \cancel{260}\ 264)$	$91 \cdot 109^{-17k}$ $(mod\ \cancel{257}\ 269)$	$210 \cdot 109^{-17k}$ $(mod\ \cancel{257}\ 269)$	109^{17k} $(mod\ \cancel{257}\ 269)$
0	1	91	210	1
1	109	45	228	8
2	45	241	163	64
3	63	131	54	243
4	142	50	74	61
5	145	208	211	219
6	203	26	60	138
7	69	205	142	28
8	258	261	85	224
9	146	268	246	178
10	43	168	98	79
11	114	21	214	94
12	52	238	94	214
13	19	97	79	98
14	188	113	178	246
15	48	115	224	85
16	121	48	28	142

(2) Find all solutions to the following equations. A table of powers of the primitive root 2 is given to help you in your calculations.

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2^k $(mod 61)$	2	4	8	16	32	3	6	12	24	48	35	9	18	36	11
k	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
2^k $(mod 61)$	22	44	27	54	47	33	5	10	20	40	19	38	15	30	60
k	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
2^k $(mod 61)$	59	57	53	45	29	58	55	49	37	13	26	52	43	25	50
k	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
2^k $(mod 61)$	39	17	34	7	14	28	56	51	41	21	42	23	46	31	1

(a) $22x \equiv 31$ $(mod\ 61)$ $\Longrightarrow 2^{16} \cdot 2^{y} \equiv 2^{59}$ $(mod\ 61)$ $\quad 16 + y \equiv 59 \ (mod\ 60)$

(b) $10x^7 \equiv 35$ $(mod\ 61)$

(c) $10x^6 \equiv 35$ $(mod\ 61)$

(d) $x^2 + 26x \equiv 10$ $(mod\ 61)$

(e) $x^2 + 13x \equiv 20$ $(mod\ 61)$

(f) $x^2 + 13x \equiv 10$ $(mod\ 61)$

(g) $55^x \equiv 2$ $(mod\ 61)$

$x^2 + 26x + 169 \equiv 10 + 169$

$(x + 13)^2$

$x^2 + 13x + 61x + 37^2 \equiv 20 + 37^2$

$(x - 24)^2 \equiv x^2 - \overset{74x}{48x} + 24^2 \equiv 20 + 24^2$

$37^2 \equiv 27$ because $37 \equiv 2^{31}$

$37^2 \equiv 2^{78} \equiv 2^{15} \equiv 27$

to compute common key

$$210^{17\cdot 16+15} \equiv \left(109^{4+7\cdot 17}\right)^{17\cdot 16+15} \pmod{257}$$

$$\equiv \left(109^{123}\right)^{287} \equiv 109^{35301} \checkmark \pmod{\overset{269}{\cancel{257}}}$$

$$210\cdot 109^{-17\cdot 7} \equiv 109^{4} \qquad \equiv 109^{229} \times \pmod{\overset{269}{\cancel{257}}}$$

$$210 \equiv 109^{4+7\cdot 17}$$

$$a^{0} \equiv 1 \equiv a^{268} \pmod{269}$$

$$\cancel{a^{\boxed{0}} \equiv 1 \equiv a^{256} \pmod{257}}$$

$$\cancel{35301 = x\,256 + 229}$$

$$229 = 17\cdot 13 + 8$$

$$109^{229} \equiv 109^{17\cdot 13}\cdot 109^{8} \equiv 98\cdot 258 \pmod{257}$$

$p = (p_1\ p_2\ p_3)$

$q = (q_1, q_2, q_3, q_4)$

p_1	p_2	p_3	p_1	p_2	p_3	p_1	p_2	p_3						
0	20	15	0	20	15	0	20	15	0	20	15	0	20	15

q_1	q_2	q_3	q_4	q_1	q_2	q_3	q_4							
7	2	14	5	7	2	14	5	7	2	14	5	7	2	14

Unicity distance # of keys $= 26^{p+q-1}$

R:	7	22	3	5	1	17	14	25	22	2	8	20	7	22	~~24~~ 5
P:	0	13	0	17	19	8	18	19	~~14~~ 13	4	21	4	17	17	4
	A	N	A	R	T	I	S	T	N	E	V	E	R	R	E
C:	7	9	3	22	20	25	6	18	9	6	3	24	24	13	7
	H	J	D	W	U	Z	G	S	J	G	D	Y	Y	N	H

A	0	F	5	K	10	P	15	U	20	Z	25
B	1	G	6	L	11	Q	16	V	21		
C	2	H	7	M	12	R	17	W	22		
D	3	I	8	N	13	S	18	X	23		
E	4	J	9	O	14	T	19	Y	24		

more

FMCME EPQMO AVMJJ KNNM

ElGamal Public Key System

To send a message X to **Bob** using his public key β, **Alice** chooses at random a secret number S_A in the interval $\{1, \ldots, p-1\}$, and sends the pair

$$(Y, Z)$$

where

$$Y := a^{S_A} \mod p, \quad \text{and} \quad Z := X\,\beta^{S_A} \mod p$$

Bob can then get X back using his secret exponent S_B:

$$X \equiv Z\,(Y^{S_B})^{-1} \mod p.$$

In this, we can consider that Y is used to "encode" S_A.

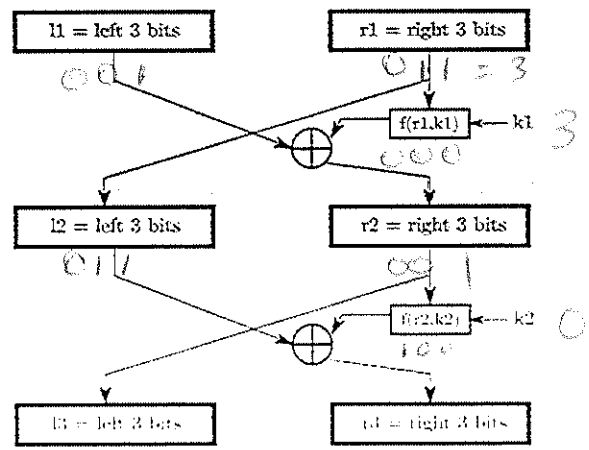
Recall D.H. S_A & S_B

Compute a^{S_A} & a^{S_B}

common key $(a^{S_A})^{S_B} \equiv (a^{S_B})^{S_A}$

0	000000	0	1	000001	1	2	000010	2	3	000011	3	4	000100	4	5	000101	5
6	000110	6	7	000111	7	8	001000	8	9	001001	9	A	001010	10	B	001011	11
C	001100	12	D	001101	13	E	001110	14	F	001111	15	G	010000	16	H	010001	17
I	010010	18	J	010011	19	K	010100	20	L	010101	21	M	010110	22	N	010111	23
O	011000	24	P	011001	25	Q	011010	26	R	011011	27	S	011100	28	T	011101	29
U	011110	30	V	011111	31	W	100000	32	X	100001	33	Y	100010	34	Z	100011	35
.	100100	36	a	100101	37	b	100110	38	c	100111	39	d	101000	40	e	101001	41
f	101010	42	g	101011	43	h	101100	44	i	101101	45	j	101110	46	k	101111	47
ℓ	110000	48	m	110001	49	n	110010	50	o	110011	51	p	110100	52	q	110101	53
r	110110	54	s	110111	55	t	111000	56	u	111001	57	v	111010	58	w	111011	59
x	111100	60	y	111101	61	z	111110	62	,	111111	63						

A Feistel cipher is used according to the following diagram encrypting each letter of a message separately. The left and right 3 bits correspond to a number between 0 and 7. The function $f(r,k) = (r+k)^2 + 3r + k \ (mod\ 8)$ is used in the Feistel cipher with $k_1 = 3$ and $k_2 = 0$ to encrypt a three letter word. Find the binary representations of $r_1, \ell_1, f(r_1,k_1), r_2, \ell_2, f(r_2,k_2)$ and the plaintext for the cyphertext FoQ (these correspond to l_3 and r_3 in the diagram).



000 = 0
001 = 1
010 = 2
011 = 3
100 = 4
101 = 5
110 = 6
111 = 7

First letter

ℓ_1: 001 r_1: 011 $f(r_1,k_1)$: 000

ℓ_2: 011 r_2: 001 $f(r_2,k_2)$: 100

Second letter

ℓ_1: r_1: $f(r_1,k_1)$:

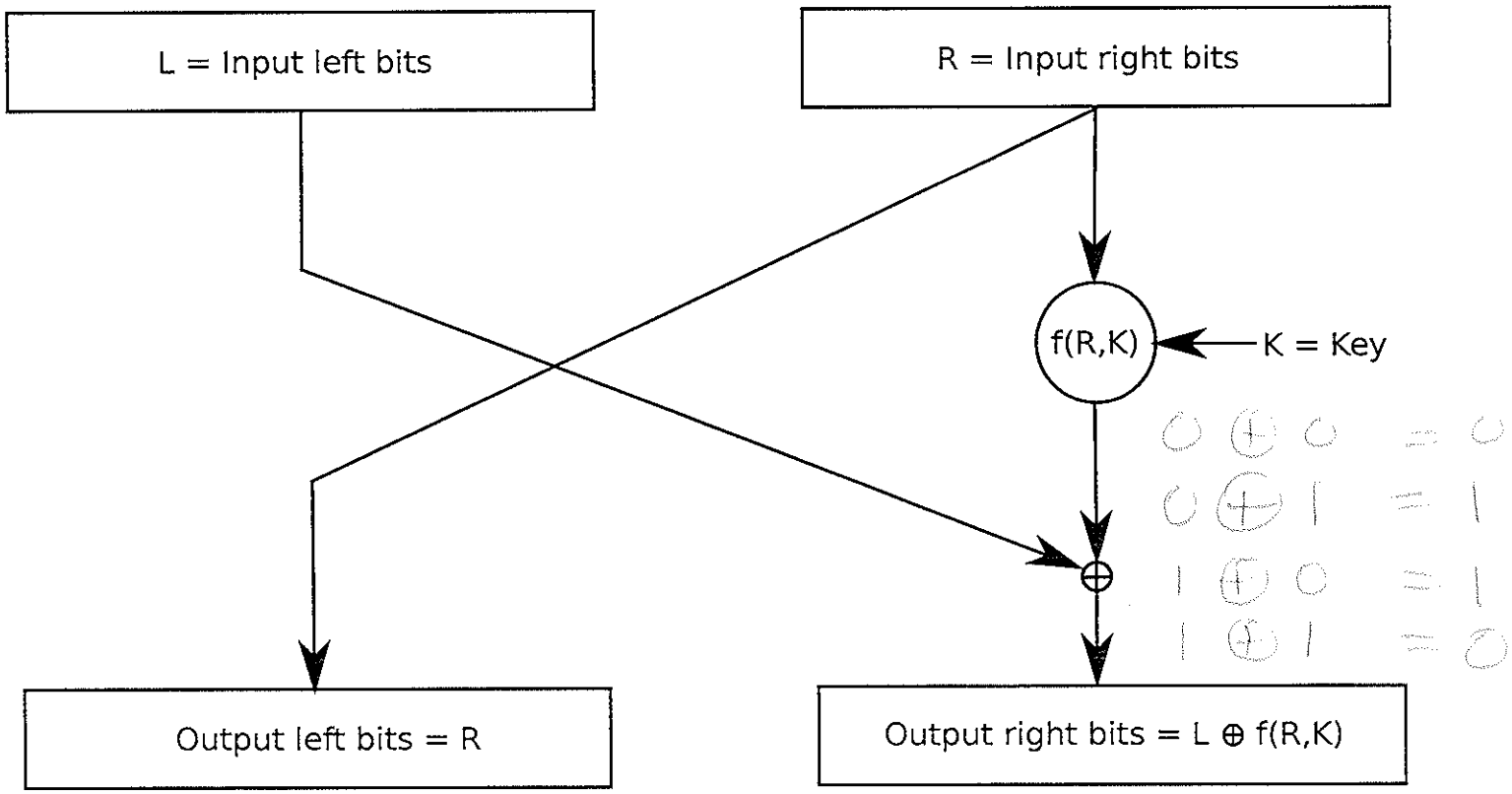
ℓ_2: r_2: $f(r_2,k_2)$:

Third letter

ℓ_1: r_1: $f(r_1,k_1)$:

ℓ_2: r_2: $f(r_2,k_2)$:

Feistel cypher



Given input in binary form, break it into LEFT and RIGHT bits (usually in half)

The right bits are transferred over to the left bits for output and the left bits are XORed with some function of the right bits and the key.