Solving Congruences

k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8	5	10	9	7	3	6	1

Example 1: Solve $9x = 5 \bmod 11$.
Letting $x = 2^y$, we have

$$2^{6+y} = 2^6 2^y = 9x = 5 = 2^4 \mod 11$$

and

$$2^{6+y} \equiv 2^4 \pmod{11}$$

$$6 + y = 4 \mod \underset{10}{\underset{\shortparallel}{\varphi(11)}}.$$

Therefore

$$y = 8 \quad \Rightarrow \quad x = 2^8 = 3.$$

Example 2: Solve $7^x = 5 \bmod 11$.
Since 2 is a primitive root, we have

$$(2^7)^x = (2^7)^x = 7^x = 5 = 2^4 \mod 11$$

Therefore

$$2^{7x} \equiv 2^4 \pmod{11}$$

$$7x = 4 \mod \varphi(11) \quad \Rightarrow \quad x = 2.$$

Note: $7 \cdot 3 \equiv 1 \pmod{10}$

$$x \equiv 3 \cdot 7x \equiv 3 \cdot 4 \equiv 2 \pmod{10}$$

ElGamal Public Key System

Bob's public key $\beta = a^{S_B} \pmod p$

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.

$$((Y)^{S_B})^{-1} \equiv ((a^{S_A})^{S_B})^{-1} \equiv (a^{S_A \cdot S_B})^{-1} \pmod p$$

$$Z \equiv X \cdot (a^{S_B})^{S_A} \equiv X \cdot a^{S_A \cdot S_B} \pmod p$$

Public Key Exchange: An Example

$\phi(37) = 36$

Powers of 2 mod 37

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^s	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36

s	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
2^s	35	33	29	21	5	10	20	3	6	12	24	11	22	7	14	28	19	1

$rx \equiv c \pmod{36}$ $\quad (2^r)^x \equiv 2^c \pmod{37}$ has a solution if r is relatively prime to $\phi(m)$

Powers of 17 mod 37

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
17^s	17	30	29	12	19	27	15	33	6	28	32	26	35	3	14	16	13	36

s	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
17^s	20	7	8	25	18	10	22	4	31	9	5	11	2	34	23	21	24	1

Say that *Alice* and *Bob* wish to communicate after agreeing on on a public modulus 37 and a primitive root 17. *Alice* also chooses a secret key 9 and so she sends $17^9 \equiv 6 \ (mod\ 37)$ to *Bob*. At the same time *Bob* chooses 10 as his secret key and so he sends $17^{10} \equiv 28 \ (mod\ 37)$ to *Alice*. *Alice* and *Bob* do not know each others secret keys but they *do* know $17^{\text{secret key}} \ (mod\ 37)$.

The common key to *Alice* and *Bob* is

$$\boxed{6^{10} = 17^{9\times 10} = 28^9 \bmod 37}$$

$17^{36} \equiv 1 \pmod{37}$

$17^{90} \equiv 17^{2\cdot 36+18} \equiv 36 \pmod{37}$

Example: $p = 53$ and $a = 3$. We wish to solve

$$3^x = 41 \ (mod 53).$$

$a^{-m} \equiv 14^8$

- $m = \lceil \sqrt{\phi(53)} \rceil = 8$ and $3^{-8} \equiv 24 \ (mod\ 53)$.
- Now $41 \cdot 24^i \ (mod\ 53)$.

$41 \cdot 3^{-8}$

i	$3^i \ (mod\ 53)$
0	1
1	3
2	9
3	27
4	28
5	31
6	40
7	14

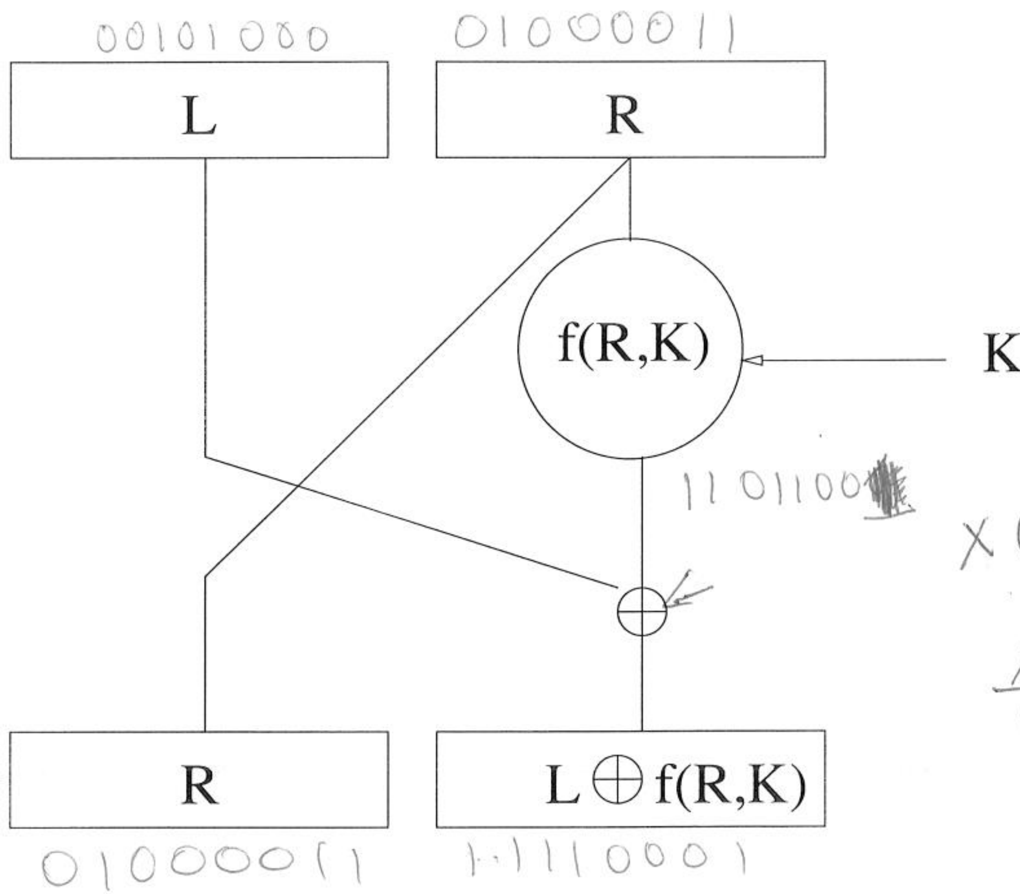
i	$41 \cdot 24^i \ (mod\ 53)$
0	41
1	30
2	31
3	2
4	48
5	39
6	35
7	45

$3^{16} \cdot 3^5 \equiv 41$

- Conclusion: $3^{2 \cdot 8+5} \equiv 3^{21} \equiv 41 \ (mod\ 53)$

$3^5 \equiv 41 \cdot 24^2 \equiv 41 \cdot (3^{-8})^2 \equiv 41 \cdot 3^{-16} \ (mod\ 53)$

Feistel Cipher



= addition mod 2

$x \oplus y$ = "exclusive" OR

x	y	$x \oplus y$
0	0	0
1	0	1
0	1	1
1	1	0

$$
\begin{array}{r}
011011110100 \\
\oplus\ 100000111011 \\
\hline
111011001111 \\
\oplus\ 100000111011 \\
\hline
011011110100
\end{array}
$$

Selection Function S_1

		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00 ≡	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01 ≡	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10 ≡	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
11 ≡	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

10

Example: 110100

- Use first and last digit as row index: 10 (base 2) = 2
- Use middle four digits as column index: 1010 (base 2) = 10
- The number 9 appears in row 2, column 10
- 9 = 1001 (base 2)

$$S_1(110100) = 1001$$