Primitive Roots

Definition: Given a prime p, an integer a is said to be a *primitive root* mod p if the numbers

$$a^1, a^2, a^3, \ldots, a^{p-1}$$

are all distinct mod p.

Example 1: 2 is a primitive root mod 11.

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

Example 2: 3 is *not* a primitive root mod 11.

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

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

$$6 + y = 4 \mod \varphi(11).$$

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

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

Therefore

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

Diffie-Hellman Public Key Exchange

1. People $P_1, P_2, \ldots P_k$ agree on a modulus p in which they agree to do their calculations.

2. They also agree on a common base, a, which must be a primitive root of p

3. Each person P_i secretly selects a number, S_i, from 1 to $p-1$ and publicly announces the value $\beta_i = a^{S_i} \bmod p$.

Obtaining A Common Key

If P_i and P_j wish to communicte secretly, they create a common secret key, $K_{i,j}$, using the following method:

a) P_i takes P_j's public number β_j and raises to his secret number S_i.

$$\beta_j^{S_i} = a^{S_j \times S_i} \mod p$$

b) P_j takes P_i's public number β_i and raises to his secret number S_j.

$$\beta_i^{S_j} = a^{S_i \times S_j} \mod p$$

Now P_i and P_j both have the number

$$\boxed{K_{i,j} = a^{S_i \times S_j} \mod p,}$$

known to nobody else and neither person has given away their private key.

Public Key Exchange: An Example

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

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

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

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.

Discrete Log Problem

The security of a Public Key Exchange rests in the difficulty of what's known as the Discrete Logarithm Problem.

$$\boxed{y = \log_a x \bmod p \quad \Leftrightarrow \quad a^y = x \bmod p}$$

Problem: Given x, find $y = \log_a x \bmod p$.

This is simple given a table of powers for a primitive root mod p. However, when p is large, say 150 digits, this method becomes unreasonable.

The Discrete Logarithm Problem is to Public Key Exchange as Factoring is to RSA