a & $\beta \, (:= a^{S_B} \mod p)$ are public for Bob

primitive root.

S_B is secret

(S_A is Alice's secret

$a^{S_A} \pmod p$ is Alice's public

D-H was share $\beta^{S_A} \equiv (a^{S_A})^{S_B} \pmod p$)

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

"Z" = cyphertext

(Y, Z)

Bob knows how to use Y to decrypt "Z"

where

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

special key that only Bob can use

message

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.

Note $Y^{S_B} \equiv (a^{S_A})^{S_B} \equiv (a^{S_B})^{S_A} \equiv \beta^{S_A} \pmod p$

which Bob can calculate using his secret key

If B knows β^{S_A} then

$$Z \cdot (\beta^{S_A})^{-1} \equiv X \beta^{S_A} \cdot (\beta^{S_A})^{-1} \equiv X \pmod p$$

$a = 2 \qquad p = 17$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2^n	2	4	8	16	15	13	9	1								

mod 17

2 is not a primitive root

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^n	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

3 is a primitive root

Bob has public key $\beta = 8 \equiv 3^{s_B}$
$\Rightarrow s_B = 10$

Alice sends $(Y, Z) = (12, 10) \qquad 12 \equiv 3^{s_A}$

Bob calculates $12 \cdot (10^{s_B})^{-1} \equiv 12 \cdot 9 \equiv 6 \pmod{17}$

$$12 \cdot ((3^3)^{10})^{-1} \equiv 12 \cdot (3^{30})^{-1} \equiv 12 \cdot 3^{-14} \equiv 12 \cdot 3^2$$
$$\equiv 3^{13} \cdot 3^2 \equiv 3^{15}$$

Bob's secret key is $\underline{10}$
Alice's secret key is $\underline{13}$

$$\gamma^x \equiv (3^{10})^x \equiv 3^{10x}$$

Baby step/Giant step method

Goal: Solve $a^x \equiv b \ (mod\ n)$.

Idea: Find $a^i \equiv ba^{-j} \ (mod\ n)$ by searching through a small enough space of possible i and j.

Idea make a table of a^i & ba^{-j}
if I find i & j s.t. $a^i \equiv ba^{-j} \pmod{n}$
then $a^{i+j} \equiv b \pmod{n}$

Fix $m = \left\lceil \sqrt{(\phi(n))} \right\rceil$ then find $c \equiv a^{-m} \ (mod\ n)$.

Next calculate a table of $a^i \ (mod\ n)$ for $0 \leq i < m$ and then calculate $bc^j \ (mod\ n)$ for $0 \leq j < m$ until you find one of these values in the table.

Solution: When we find $a^i \equiv bc^j \ (mod\ n)$ then we have $a^{i+mj} \equiv a^i c^{-j} \equiv b \ (mod\ n)$.

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

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

ba^{-jm} for $0 \le j \le m$

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

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

i	$41 \cdot 24^i \ (mod\ 53)$
0	41
1	30
2	31 $\equiv 41 \cdot 24^2 \equiv 41 \cdot 3^{-16}$
3	2
4	48
5	39
6	35
7	45

$41 \equiv 3^{5+16} \ (mod\ 53)$

$\equiv 3^{21} \ (mod\ 53)$

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

$1 \le a \le p-1 \qquad a^{p-1} \equiv 1 \pmod{p}$

Theorem 3 *For any prime $p > 2$ and any integer a not equal to 0* (mod p) *we have*

$$a^{(p-1)/2} = \begin{cases} 1 & \text{if } a \in QR[p] \\ -1 & \text{if } a \notin QR[p] \end{cases}$$

Proof.

If $a = x^2$ with $x \neq 0 \bmod p$ then Fermat's theorem gives

$$(x^2)^{(p-1)/2} \equiv a^{(p-1)/2} = x^{p-1} = 1 \pmod{p}$$

Thus the first part of our assertion holds true. To prove the second part, note that the equation

$$x^{p-1} - 1 = 0 \pmod{p}$$

has exactly $p-1$ solutions in $\{1, 2, \ldots, p-1\}$ and for $p > 2$ we have the factorization

$$x^{p-1} - 1 = (x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1) \equiv 0$$

All $(p-1)/2$ elements of $QR[p]$ satisfy the first factor. Therefore the other $(p-1)/2$ solutions must satisfy

$$x^{(p-1)/2} + 1 = 0.$$

Legendre Symbol

For a prime p

not a fraction

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in QR[p] \\ -1 & \text{if } a \notin QR[p] \\ 0 & \text{if } gcd(a,p) > 1 \end{cases}$$

$L(a,p)$

Then for a relatively prime to p, we have

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p$$

Because of the last theorem.

Hence

$$(ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{\frac{p-1}{2}} b^{(p-1)/2} \pmod{p}$$

Theorem 4 (Quadratic Reciprocity) *For any two primes p and q we have*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

$\cancel{J(4, 12)}$

$\cancel{J(7, 12) = J(12 \bmod 7, 7)(-1)}$

$$J(7, 15) = J(15 \bmod 7, 7)(-1)^{21} \equiv -J(1, 7) = -1$$

$$\text{by def} = \left(\frac{7}{5}\right)\left(\frac{7}{3}\right) \equiv \left(\frac{2}{5}\right)\left(\frac{1}{3}\right) \equiv (-1)\cdot(1) \equiv -1$$

$$J(5, 77) = J(77 \bmod 5, 5)(-1)^{76\cdot 4/4} = J(2,5) \equiv \underbrace{J(1,5)}(-1)^{(25-1)/8}$$

$$\equiv \underline{1}\cdot(-1) = -1$$

$$= \left(\frac{5}{7}\right)\left(\frac{5}{11}\right) = (-1)(+1) = -1$$

$1^2 = 1,\ 2^2 = 4,\ 3^2 = 2 \pmod 7$

$1^2 = 1 \quad 2^2 = 4 \quad 3^2 = 9 \quad 4^2 = 5 \pmod{11}$

Primality Testing

The Jacobi symbol allows us to test for primality of n without carrying out its factorization.

If n is prime then

$$\left(\frac{a}{n}\right) \leftarrow \text{if } n \text{ prime}$$

$$J(a,n) = a^{(n-1)/2} \mod n$$

Thus if this identity fails to hold for any value of a in $[1, n-1]$ we can certainly conclude that n is not a prime!

Theorem 5 *If n is not a prime then for more than one half the integers in $\{1, \ldots, n-1\}$ one of the following two tests will fail*

$$J(a,n) = a^{(n-1)/2} \qquad \gcd(a,n) = 1$$

Jacobi Symbol

We start with the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in QR[p] \\ -1 & \text{if } a \notin QR[p] \end{cases}$$

and for

extension of Legendre symbol to all integers.

$$n = p_1 p_2 \cdots p_k$$

we set

$$J(a, n) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$

Jacobi symbol

However, for n odd, we have

$$J(a, n) = \begin{cases} 1 & \text{if } a = 1 \\ J(a/2, n)(-1)^{(n^2-1)/8} & \text{if } a \text{ is even} \\ J(n \mod a, a)(-1)^{(n-1)(a-1)/4} & \text{if } a > 1 \text{ and odd} \end{cases}$$

Recursive method for computing Jacobi symbol.