Elgamal based cryptography

1) Prime Number p
   Generator g
   $p < g$; $GCD(p, g) \Rightarrow 1$

2) private key $2 \leq d \leq p-2$

3) public key $e \Rightarrow g^d \bmod p$

4) $GCD(K, p-1) \Rightarrow 1$ random number K

5) $y_1 \Rightarrow g^k \bmod p$

6) $y_2 \Rightarrow \left[K^{-1} (\text{message hash value} - dy_1) \right] \bmod (p-1)$

} Generating digital signature

7) hash value $\Rightarrow$ Hash (message)

8) $V_1 \Rightarrow \left(g^{\text{hash value}} \right) \bmod (p)$

9) $V_2 \Rightarrow \left[e^{y_1} (y_1)^{y_2} \right] \bmod (p)$

} Authentication.

Given

Message $\Rightarrow$ 4

prime number $p \Rightarrow 19$

generator $g \Rightarrow 10$

private key $d \Rightarrow 16$

random number $k \Rightarrow 5$

hash value $\Rightarrow 14$

private key

$2 \leq d \leq p-2$

$2 \leq 16 \leq 18$ ✓

public key

$e \Rightarrow g^d \bmod p$

$\Rightarrow 10^{16} \bmod 19$

$e \Rightarrow 4$

$10^{16} \bmod 19$ (Modular Exponentiation)

$10^{2} \bmod 19 \Rightarrow 5$

$10^{4} \bmod 19 \Rightarrow (5*5) \Rightarrow 25 \,\%\, 19 \Rightarrow 6$

$10^{8} \bmod 19 \Rightarrow (6*6) \Rightarrow 36 \,\%\, 19 \Rightarrow 17$

$10^{16} \bmod 19 \Rightarrow (17*17) \,\%\, 19 \Rightarrow 4$

Digital signature

Random number $\quad GCD(k, p-1) \Rightarrow 1$

$GCD(5, 18) \Rightarrow 1$

$y_1 \Rightarrow g^{k} \bmod p$

$y_1 \Rightarrow 10^{5} \bmod 19 \Rightarrow 3$

$\boxed{y_1 \Rightarrow 3}$

$$y_2 \Rightarrow \left(k^{-1} \left[\begin{matrix} \text{hash value} \\ \text{message} \end{matrix} - d y_1 \right] \right) \,\%\, (p-1)$$

$$\Rightarrow \left[5^{-1} \left(14 - 16(3) \right) \right] \,\%\, 18$$

$$\Rightarrow \left[5^{-1} (-34) \right] \,\%\, 18$$

$$\Rightarrow \left(5^{-1} \,\%\, 18 \right) * \underbrace{\left(-34 \,\%\, 18 \right)}$$

$18 - (34 \,\%\, 18) \Rightarrow 18 - 16 \Rightarrow 2$

~~$18 - 8 \Rightarrow 10$~~

$5^{-1} \% 18$

$\hookrightarrow (5 * x) \% 18 \Rightarrow 1$

$18x + 5y = GCD(18, 5)$

$y = y_1 - q y_2$

q	r_1	r_2	r	y_1	y_2	y
3	18	5	3	0	1	-3
1	5	3	2	1	-3	4
1	3	2	1	-3	4	-7
2	2	1	0	4	-7	18
		1	0		-7	18

$0 - 3(1) \Rightarrow -3$

$1 - 1(-3) \Rightarrow 4$

$-3 - 1(4) \Rightarrow -7$

$4 - 2(-7) \Rightarrow 18$

$5^{-1} \% 18 \Rightarrow 11$

$-7 \bmod 18$

$18 - (7 \bmod 18)$

$18 - (7) \Rightarrow 11$

$y_2 \Rightarrow (11 * 2) \Rightarrow 22 \% 18$

$y_2 \Rightarrow 4$

Digital signatures:

$y_1 \Rightarrow 3$

$y_2 \Rightarrow 2$

Verification

$V_1 \Rightarrow (g^{hash\ value}) \% p$

$\Rightarrow 10^{14} \% 19 \Rightarrow (10^{2+4+8} \% 19) \Rightarrow 510 \% 19 \Rightarrow 16$

$V_1 \Rightarrow 16$

$V_2 \Rightarrow (e^{y_1 y_1^{y_2}}) \% p \Rightarrow (4^3 3^4) \% 19 \Rightarrow 16$

$\Rightarrow (4^{\cdot} 3^{\cdot}) \% 19 \Rightarrow 2304 \Rightarrow 576 \% 19$

$V_2 \Rightarrow 16$