classmate

Date
Page

# Assignment 3

1\. Prove the correctness of Elgamal signature verification ($v_1 = v_2$)

=) If the signature $(r, s)$ to message M is valid then,

$$v_1 \equiv y^r r^s$$
$$\equiv (g^x)^r (g^k)^s$$
$$\equiv g^{xr + ks}$$
$$\equiv g^{H(M||r)}$$
$$\equiv v_2 \pmod p$$

Example:

Let $p = 467$, $g = 2$ which is primitive root of 467

secret key $x = 127$

$$y = 2^{127} \equiv 132 \pmod{467}$$

So consider Alice with

public key {467, 2, 132}

private key 127

If Alice wants to sign msg

she selects $k = 213$; note that $\gcd(213, 466) = 1$

$$r \equiv 2^{213} \equiv 29 \pmod{467}$$

Suppose hash function yeilds $H(\text{"11; Time"} || 29) = 100$

Alice needs to solve

$$123 s \equiv 100 - 127 \cdot 29 \equiv 145 \bmod 466$$

Solve

~~$123s \equiv 100 - 127 \cdot 29 \equiv 145 \pmod{466}$~~

Scanned with CamScanner

Extended euclidian

$123z \equiv 1 \pmod{466}$

$z = 431 \bmod 466$

$s = 145.431 \equiv 51 \pmod{466}$

$(r, s) = 29, 51$

$r = 29 < 467$

$v_1 = 132^{29} \cdot 29^{51} \equiv 189 \pmod{467}$

$v_2 = 2^{100} \equiv 189 \pmod{467}$

$v_1 = v_2 = 189$

2 $q = 19$ , $\alpha = 3$

$x_A = 16$ $y_A = 3^{16} \bmod 19$
$= 17$

$k = 5$ $\gcd(18, 5) = 1$

$s_1 = 3^5 \bmod 19 = 15$

$5^{-1} \bmod 18 = 11$

$s_2 = 11(14 - 240) \bmod 18$
$11(-226) = 16$

$15, 16$

$v_1 = 3^{14} \bmod 19 = 4$

$v_2 = 17^{15} \times 15^{16} \bmod 19$
$= 7 \times 6 = 4$

$v_1 = v_2$

Scanned with CamScanner

3

a) If $y_i = y_j$ for $i \neq j$, then

$$y_{i-1} \oplus x_i = y_{j-1} \oplus x_j$$

As $y_{i-1}$ and $y_{j-1}$ are known, we can deduce the value

$$x_i \oplus x_j = y_{i-1} \oplus y_{j-1}$$

b) Using birthday paradox, we know that the probability of getting a collision when we have $n = \theta\sqrt{2^{64}}$ blocks at disposal is approximately equal to $1 - e^{-\theta^2/2}$