MATH 178 Homework #15

Tamir Enkhjargal

June 2019

My Color: Red. My Partner's Color: Blue

ElG 5.

$p = nextprime(10^{24}) = 1000...0007$
$g = 5$
$a_A = 2000...0069$
$H = 2067...5961$
$k = 6727...9337$
$r = g^k \bmod p = 8438...4084$
$x = k^{-1}(H + a_A r)(\text{mod} p - 1) = 1829...6413$
Therefore my public key is $(r, x, H) = (8438...4084,\ 1829...6413,\ 2067...5961)$.

My partner's signature, (r, x, H) was $(84838...4084,\ 6766...0429,\ 2067...5961)$. To verify his signature, I calculate $g^H \bmod p,\ (g^a)^r \bmod p, r^x \bmod p$.

I confirm that $g^H + ar \bmod p = r^x \bmod p = 362630633707826341655801$

ElG 6.

If Alice uses the same k to encrypt two different signatures H_1 and H_2, we know that some things are kept constant. From the original equation:

$$r \equiv g^k \bmod p \tag{1}$$
$$x \equiv k^{-1}(H + a_A r)(\text{mod} p - 1) \tag{2}$$

If Alice is keeping the same k, then Alice also has the same r. We can now set up a system of equations:

$$x_1 \equiv k^{-1}(H_1 + a_A r)(\text{mod} p - 1) \equiv k^{-1}H_1 + k^{-1}a_A r(\text{mod} p - 1) \tag{1}$$
$$x_2 \equiv k^{-1}(H_2 + a_A r)(\text{mod} p - 1) \equiv k^{-1}H_1 + k^{-1}a_A r(\text{mod} p - 1) \tag{2}$$
$$x_1 - x_2 \equiv k^{-1}(H_1 - H_2)(\text{mod} p - 1) \tag{3}$$

From here, Eve knows x_1, x_2, H_1, H_2, and p. She does not need to deal with the $FFDLP$ here, just a simple modular inversion to find k.

ECDSA 1.

The first 16 lines was setting up variable names from `ECDSA.txt`.

```
?  ellpow(E,G,H)
%17 = [Mod(35634253512680661292, 100000000000000000039), Mod(77324529282921925367,
100000000000000000039)]
?  ellpow(E,aAG,kG[1])
%18 = [Mod(41228830649142682590, 100000000000000000039), Mod(36578933883955767227,
100000000000000000039)]
?  elladd(E,%17,%18)
%19 = [Mod(19543389628484684932, 100000000000000000039), Mod(99444274481452187725,
100000000000000000039)]
?  lift(%19)
%20 = [19543389628484684932, 99444274481452187725]
?  ellpow(E,kG,x)
%21 = [Mod(19543389628484684932, 100000000000000000039), Mod(99444274481452187725,
100000000000000000039)]
?  lift(%21)
%22 = [19543389628484684932, 99444274481452187725]
?  %20
%23 = [19543389628484684932, 99444274481452187725]
```

In the end, the check is $G * H + a_A G * kG[1] \stackrel{?}{=} kG * x$, where multiplication is `ellpow` and addition is `elladd`

MAC 2.

From the previous MAC 1. problem, the end result was $= [1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0]$. This number in integer form is 46822. From CW-RSA-2, we know that my RSA private key is: $n = 1859...2729$, and $d = 1781...9173$. Also my e was given as $= 5746...7277$. To sign the hash H, we compute $H^d \bmod n = M$. This signed message M was then 1562...8946. To confirm that this is true, my partner can calculate $M^e \bmod (n) = H$, and after calculating we can confirm that $H = 46822$ again.

MAC 3.

From CW-ElG-5, we've previously found a couple of things. $p = nextprime(10^{24}) = 1000...0007$, $a_A = 2000.069$, $H = 46822$, $k = 6727...9337$. I calculate $r = g^k \bmod p$, and $x = k^{-1}(H + a_A r)(\text{mod} p - 1)$.

Therefore my signature $(r, x, H) = (8438...4084,\ 2797...1422,\ 46822)$.

My partner confirms by finding $g^H \bmod p$, $(g^a)^r \bmod p$, and then $g^H g^{ar} (\bmod p)$ and confirmed it with $r^x \bmod p$.

ElG 7.

i) From the equation $kx \equiv H + a_A r (\bmod p-1)$, the only unknown is a_A and everything else is known. Therefore Freddy can get Alice's private key.

ii) The exact problem $g^{a_A} (\bmod p) = PK$, in finding a_A is the $FFDLP$. It is very very difficult to brute-force through all exponents n to find it equal to a_A.

iii) In the equation $r^x \equiv (g^H)(PK^r)(\bmod p)$, everything is *technically* given/known. However $PK \equiv g^{a_A} (\text{mod} p)$, and it comes back to the $FFDLP$.

iv) In this equation, Freddy has two unknowns, k and a_A. He has everything else, but in a linear equation with two unknowns, there can be an infinite amount of solutions (due to some rules in Linear Algebra k and a_A are not independent variables).

v) Again, this comes back to the $FFDLP$, it is cryptographically difficult to brute force through the exponents.

vi) Exact same answer as part iv). With two unknowns, k and a_A can be any infinite pair of solutions and it will be a chance of 1/infinity for Freddy to guess the correct pair.