

LESSON 16

Review Pollard >

Remarks on Key Exchange

Digital Signatures

Protocol Hierarchies

Review Colesium Algorithms

Ex Solve $2^x \equiv 9 \pmod{13}$

$$a_0 = 2 \quad b_0 = 9$$

$$q_1 = a_0 2^{h(a_0)} = 2 \cdot 2^{h(2)} = 2 \cdot 2^2 = 2^3 = 8$$

$$q_2 = q_1 2^{h(a_1)} = 2^3 \cdot 2^{h(8)} = 2^3 \cdot 2^2 = 2^5 = 32 = 6$$

$$q_3 = q_2 2^{h(a_2)} = 2^5 \cdot 2^{h(6)} = 2^5 \cdot 2^2 = 2^7 = 11$$

$$q_4 = q_3 2^{h(a_3)} = 2^7 \cdot 2^{h(11)} = 2^7 \cdot 2^3 = 2^{10} = 88 = 10$$

$$b_0 = 9$$

$$b_1 = b_0 2^{h(b_0)} = 9 \cdot 2^{h(9)} = 9 \cdot 2^1 = 9 \cdot 2 = 18 = 5$$

$$b_2 = b_1 2^{h(b_1)} = 9 \cdot 2 \cdot 2^{h(5)} = 9 \cdot 2 \cdot 2^1 = 9 \cdot 2^2 = 10$$

$$b_2 = q_4 = 10$$

$$9 \cdot 2^2 = 2^{10}$$

$$9 = 2^8$$

$$x = 8$$

L	1	2	3	4	5	6	7	8	9	10	11	12
$h(u)$	1	2	3	2	1	2	3	2	1	2	3	2

is the hash function

2

Problem

Solve $b^x \equiv 3 \pmod{13}$

Use the hash function we used
in the example $2^x \equiv 9 \pmod{13}$

You may need to use Fermat's

Theorem, $a^{p-1} \equiv 1 \pmod{p}$

and $a^{-k} = a^{p-1-k} \pmod{p}$

Mischief on the Key Exchange

Alice picks prime p and c
with $\gcd(c, p) = 1$

She makes (c, p) public

Alice picks integer a , computes
 $x \equiv c^a \pmod{p}$

and sends x to Bob

Bob picks integer b and computes
 $z \equiv c^b \pmod{p}$

and sends z to Alice

Eve knows p, c, x and z

Eve picks d , computes

$$y = c^d \pmod{p}$$

and sends y to both Bob

and Alice, telling them it came
from the other

Eve and Bob Alice compute
 $c^{ad} = (c^a)^d \pmod{p}$. Now ~~Alice~~

Eve pretends she is Bob
using $c^{da} \bmod p$ as their
key.

Similarly, Eve and Bob
compute $c^{d^b} = (c^b)^d \bmod p$
and pretends she is Alice

Now Alice and Eve exchange
messages with Alice thinking
that Eve is Bob

They use the key $c^{da} \bmod p$

A similar result occurs
between Bob and Eve
using $c^{d^b} \bmod p$

Digital Signatures

Alice picks primes p and q
with $p \equiv 1 \pmod{q}$, $q < p$.

She picks g to be in the
group of non-zero elements
in the integers mod p .

This can be done as follows:

Pick a generator g_1 of
this group and compute

$$g = g_1^{(p-1)/q}$$

Then $g^q = g_1^{(p-1)} \pmod{p} = 1$

so g has order q (~~and hence~~
containing

Alice picks a and computes
 $A = g^a \pmod{p}$. Alice sets out
 (p, q, g, A) as her verification
key to verify her signature.

Note that a is kept secret.

Alice sends message D to Bob. She signs it as follows
She picks k , $1 < k < g$.
She computes

$$S_1 = (g^k \bmod p) \bmod q$$

$$S_2 = (D + aS_1)k^{-1} \bmod q$$

(only she can compute S_2 because of a)

Her signature is (S_1, S_2)

so $D, (S_1, S_2)$ are sent to Bob

Bob computes

$$V_1 = D S_2^{-1} \bmod q$$

$$V_2 = S_1 S_2^{-1} \bmod q$$

The check is, does

$$g^{V_1} A^{V_2} \bmod p \bmod q = S_1$$

Proof.

$$\begin{aligned}
 & g^{V_1} A^{V_2} \bmod p \bmod q \equiv \\
 & g^{D S_2^{-1}} A^{S_1 S_2^{-1}} \bmod p \bmod q \equiv \\
 & g^{D S_2^{-1}} g^{a S_1 S_2^{-1}} \bmod p \bmod q \equiv \\
 & g^{D S_2^{-1} + a S_1 S_2^{-1}} \bmod p \bmod q \equiv \\
 & g^{(D + a S_1) S_2^{-1}} \bmod p \bmod q \equiv \\
 & g^k \bmod p \bmod q = S_1.
 \end{aligned}$$

Note that only Alice can compute S_2 since only she knows a .

Ex. Alice picks $p = 23$, $g = 11$,
 $g = 2$ with $|g| = 11$ and $a = 5$

She finds $A = g^a \bmod p =$
 $2^5 \bmod 23 = 9$

Her verification key is

$$(P, g, g, A) = (23, 11, 2, 9)$$

Suppose her message is $D = 3$

She picks $k = 2$, $k^{-1} \bmod 11 = 6$

$$\text{Then } S_1 = g^k = 2^2 = 4$$

$$\begin{aligned} S_2 &= (D + a S_1) k^{-1} \bmod 11 \\ &= (3 + 5 \cdot 4) 6 \bmod 11 = 6 \end{aligned}$$

She signs D with

$$(S_1, S_2) = (4, 6)$$

$$\begin{aligned} \text{Bob finds } V_1 &= D S_2^{-1} = 3 \cdot 6 = 3 \cdot 2 \bmod 11 \\ &= 6 \end{aligned}$$

$$V_2 = S_1 S_2^{-1} \bmod g = 4 \cdot 6^{-1} \bmod 11 = 8$$

$$\begin{aligned} \text{Then } g^{V_1} A^{V_2} &= 2^6 \cdot 9^8 \bmod 23 \bmod 11 \\ &= 8 \cdot 12 \bmod 23 \bmod 11 = 4 = S_1 \end{aligned}$$

9

HIERARCHY

Given g and prime p

We have 3 protocols

I DLP Given $g^a \text{ mod } p$, find a

II DHP Given $g^a \text{ mod } p$, $g^b \text{ mod } p$,
find $g^{ab} \text{ mod } p$

III EL GAMAL Review it

Alice picks a and sends

$$(g, g^a \text{ mod } p)$$

She gets back $(g^b, g^{ab}m \text{ mod } p)$

She can find $(g^b)^{-a} g^{ab}m \text{ mod } p = m$
since she knows a .

Eve can not do that step

Abstracting, it is said that one
can solve the EL-GAMAL if given

(c_1, c_2) one can find $c_1^{-a} c_2 \text{ mod } p$

In the real EL-GAMAL

$$c_1 = g^b \quad c_2 = g^{ab}m, \text{ all mod } p$$

Suppose we can do this, solve
the abstract EL-GAMAL

In the DHP we know $g^a, g^b \text{ mod } p$

$$\text{Let } c_1 = g^b \quad c_2 = 1$$

$$c_1^{-a} c_2 = g^{-ab} \cdot 1 \text{ mod } p \text{ which we}$$

10 Say we can solve because it is the EL-GAMAL PROBLEM. Hence we can then find $g^b \pmod p$ and we have solved the DHP. Conclusion: If we can solve the EL-GAMAL, then we can solve the DHP.

Conversely, in the EL-GAMAL we know $g^a \pmod p$ and $g^b \pmod p$ and $m g^{ab} \pmod p$. Knowing how to solve the DHP, we get $g^{ab} \pmod p$.

Then $(g^b)^{-a} m g^{ab} \pmod p = m \pmod p$
(we know $(g^b)^{-a} = g^{-ab} \pmod p$ since we know $g^{ab} \pmod p$)

So, if we can solve the DHP, we can solve the EL-GAMAL.

Conclusion

The DHP and EL-GAMAL are equally hard. The DLP, as we have seen, is at least as hard as the DHP, so it could be the hardest. Could be because we don't know if solving one of the others will solve the DLP.