Exam Corrections

1

Bob and Alice which to use Diffie-Hellman key exchange, using the prime number $p = 31$ and base $g = 3$. To simplify your work, here is a table of the powers of 3:

i	3^i
1	3
2	9
3	27
4	19
5	26
6	16
7	17
8	20
9	29
10	25
11	13
12	8
13	24
14	10
15	30
16	28
17	22
18	4
19	12
20	5
21	15
22	14
23	11
24	2
25	6
26	18

i	3^i
27	23
28	7
29	21
30	1

a

Alice chooses secret key $a = 7$. What number A does she send to Bob?

✓ **Answer**

$A = g^a \pmod p$

$A = 3^7 = 27$

b

If Bob sends Alice the number $B = 13$, what is their shared secret key K?

✓ **Answer**

$B = g^b$

$K = B^a = g^{ab}$

$13 = 3^{11}$

$K = 3^{(11)(7)} = 3^{77} = 3^{17} = 22$

c

Of course, the numbers above are tiny. In a realistic setting, given data (p, g, A, B, K) what precisely is meant by the Diffie-Hellman Decision Problem?

✓ **Answer**

You cannot guess g^a and g^b from g^{ab} when $\pmod p$

2

Bob and Alice agree to communicate using ElGamal Public Key Encryption. They agree on a prime p and a base g. Alice has private key a and public key $A = g^a \pmod p$.

a

Bob wants to send message m to Alice. He chooses a random number k. What ciphertext does he send to Alice?

> ✓ **Answer**
> $\langle c_1, c_2 \rangle$
> $c_1 = g^k$
> $c_2 = mA^k$

b

When Alice receives the ciphertext from Bob, how does she decrypt it?

> ✓ **Answer**
> $A^k = g^{ka} = c_1^a$
> $m = c_2(A^k)^{-1} = c_2(c_1^a)^{-1}$
>
> $c_2(c_1^a)^{-1} = m$

c

Can Eve successfully attack this system using the Known Plain-text Attack? Why or why not?

> ✓ **Answer**
> No, because the nonce will be different for every message

3

The polynomial $x^5 + x^2 + 1$ is irreducible over $\mathbb{F}_2$.
Let $\mathbb{F}_{32} = \mathbb{F}_2[X]/(X^5 + X^2 + 1)$ with $\alpha = [X]$

Any element $\beta = a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$ of the field can be represented by a binary string $a_4a_3a_2a_1a_0$. For example, α is represented by the string 00010.

a

If $\beta_1 = \alpha^4 + \alpha$ and $\beta_2 = \alpha^2 + \alpha + 1$, compute the binary string representing $\beta_1\beta_2$.

> ✓ **Answer**
> $\beta_1\beta_2 = (\alpha^4 + \alpha)(\alpha^2 + \alpha + 1)$
> $= \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$
> $= (\alpha + 1)(\alpha^2 + 1) + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$

$= \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$
$= \alpha^4 + 1$
$\to 10001$

b

Compute the binary string representing α^{11}.

✓ **Answer**
α^{11}
$= (a^5)^2 \alpha$
$= (\alpha^2 + 1)^2 \alpha$
$= (\alpha^4 + 1)\alpha$
$= \alpha^5 + \alpha$
$= \alpha^2 + \alpha + 1$
$\to 00111$

c

Is the polynomial $x^5 + x^2 + 1$ primitive? Briefly explain your answer.

✓ **Answer**
Yes, as in order for it to be non-primitive, it must be able to loop to 1 for some value $n < 31$ such that $\alpha^n = 1$.

This is impossible as 31 is prime and $\alpha^{31} = 1$
There cannot be an n that divises 31 where there is an integer b such that $31 = bn$

4

What is the key idea underlying each of the following:

a

The Pohlig-Hellman Algorithm?

✓ **Answer**
With $y = g^x \pmod{p}$ given y, g, p to find x,

With $p_{1 \ldots} p_n$ as the factors of $\varphi(p)$
We may derive equations that solve for x in each $\pmod{p_i}$

We may then use the Chinese Remainder Theorem to reconstruct the original $x \pmod{\varphi(p)}$

b

The Pollard Rho Algorithm?

✓ Answer

In order to find factors of a large number N:

We are likely to find a factor for some large value N by computing its gcd with a series of numbers defined as the following:

For $i \in [1, 2, ...]$ calculate $\gcd(2^{i!} - 1, N)$

If this number is not 1, then you have found a factor of N

c

Entropy?

✓ Answer

For some variable X,

Entropy H is defined as $H(X) = \sum_{x \in X} -P(X = x) \log_2(P(X = x))$

This represents the number of bits of uncertainty per bit of input.

The more entropy a cryptosystem produces, the less likely someone is able to statistically analyze its encrypted secrets and derive the secret.