Homework#9

***1.Can you propose a DSA scheme with ECC and the extended Galois field?***

**Key Generation**

* Using Elliptic curve (EC) which is

+xy +a+b mod P(x), where b 0

P(x) is an irreducible polynomial of

Primitive A ()

* The private key d is a random number between cyclic group

*0 d q*

*Where q is the # of elements in cyclic group*

* Compute

*B = d. A 🡪* *B ()*

*Public:(m,a,b,q,A,B)*

*Private Key: d*

**Signature**

* Choose a random ephemeral integer

0 <q

* Compute R =  .A 🡪 R () 🡪 r =
* Compute S (h(x) + d. r) mod q

is the inverse of KE mod q

**Verification**

* Compute: w mod q
* Computer: w. h(x) mod q
* Computer: w. r mod q
* Compute: P = A + B 🡪 *P ()*

*If: r mod q 🡪 valid signature*

*If: r mod 1 🡪 invalid signature*

***2. Can you propose a simple example demonstrating a DSA with ?***

**Key Generation**

P(x) is an irreducible polynomial of , at here

*P(x) = + x + 1, a = ,b=1, q=16*

*Primitive A () = ()*

*d = 5 =*

*B = d. A = ()*

**Signature**

Choose a random ephemeral integer = 3

R = .A = (*) 🡪 r = = = 1100 = 12*

Sign has message h(x) = 7

S (7+ 5 x 12) x 11 mod 16

S 737 mod 16

S 1 mod 16

(r,s) = (,1)

**Verification**

w mod 16

mod 16

17 mod 16

17. 7 mod 16 1.7 mod 16 7 mod 16

17. 12 mod 16 1.12 mod 16 12 mod 16

P = A + B 🡪 *P () = 7A+12B*

*=67P + 3P = ()*

**It is verified**