**Exam Questions INF143A**

**Finite fields:**

F2^n

F2^6 means (0,1,1,0,0,1) with some bits 0 and 1

To construct finite field we need to use a irreducible polynomial of degree 6 if n = 6.

Smallest finite field / irreducible polynomial = F2

An irreducible polynomial has no roots in F2

**Addition** and **subtraction** in finite field is just XOR:

(0,1,1,0,0,1)

(1,1,1,0,0,1

= (1,0,0,0,0,0)

Irreducible polynomial / irr of degree 6 = x^6 + x + 1

**Multiplication** with irr:

0 1 1 0 0 1

x + x^2 + x^5

1 1 1 0 0 1

1 + x + x^2 + x^5

(x + x^2 + x^5) \* (1 + x + x^2 + x^5) = x + x^4 + x^5 + x^10

(check out lecture for full calculation)

Represented in 6 bits -> X^10 = x^5 + x^4 ->

**Differential uniformity:**

You have unction F, x1 and x2

Perform x1 XOR x2 = A

Feed x1 -> F = y1 and x2 -> F = y2

Perform y1 XOR y2 = B

Find x2 such that x1 XOR x2 = A:

= x1 XOR x1 XOR x2 = x1 XOR A #XOR both sides with x1

= x1 cancels out and you get = x2 = x1 XOR A

Check out lecture

**DHKE – Diffie Hellman Key Exchange**

Find a large prime p

Zp = {0,0,2,…, p-1}

You have a generator g

Take Z7 = {0,1,2,3,4,5,6}

2^1 mod 7 = 2

2^2 mod 7 = 4

2^3 mod 7 = 1

2^4 mod 7 = 2 (looped), not a generator

3^1 mod 7 = 3

3^2 mod 7 = 2

…

3^6 = 1

Using 3 we find 1,2,3,4,5,6 (all numbers in Z7 except 0)

3 is a generator

Alice:

a

A = g^a

Bob:

b

B = g^b

A is sent to bob, B is sent to Alice

B^a = (g^b)^a = g^ab

A^b = (g^a)^b = g^ab

They end up with the same key/value g^ab

**Hash functions**

Take input or arbitrary length and always give output with same fixed size

Pre-image resistance: if you see the output of the hash function, you should not be able to guess what the input is. h(x) = y, if you know y, you should not be able to find x.

Collision resistance: You should not be able to find x1 and x2 which satisfies h(x1) = h(x2) (same hashes y). You know x1 and h(x1) and x1 is fixed. Your goal is to find an unknown x2.

Strong collision resistance: Same as collision resistance but x1 is not fixed here and is unknown. You can find either x1 or x2 and be successful.