Applied Cryptography

Unit 1

In theory applied cryptography is more efficient, modern cryptography is more mathematically secure

Modular arithmetic

=c (3 lines, congruent)

a = r Mod m not the same as (a equals r Mod m)

1. Remainder of a/m same as that of r/m (smallest positive remainder)
2. a = n \* m + r
3. m / a-r

17 =c 10 (mod 7)

1. 17/7 remainder = 3 10/7 remainder = 3
2. 17 = n \* 7 + 10 (n = 1)
3. 7 / 17 -10 = 7/7 , 7 is divisible by 7

-------------------------------------------------------------------

(x mod m + y mod m) (mod m)

(r1) (r2)

x = i \* m + r1

y = j \* m + r2

x + y = (i \* j) \* m + r1 + r2

anything times what is being modulo, remainder will be 0, m = 7 i = 2 j = 4; 2\*4 = 8, 8\*7 = 56

(r1 + r2) mod m

-------------------------------------------------------------------