Additive Cipher

Multiplicative Cipher

**Affine Cipher:**

C=(P \* k1 +k2) mod 26

P=((C- k2 ) \* k1-1 )mod 26

K1=001 K2=010

Ex: “hello” with the key (7,2) using affine cipher

h—7 e-4 l-11 l-11 0-14

=(7 \* 7 +2) mod 26 =25-Z

=(4 \* 7 +2) mod 26= 4---E

= (11 \* 7 +2) mod 26= 1—B

1---B

=(14 \*7 +2) mod 26= 22---W

hello---- ZEBBW

Decryption:

=((25 +(-2)) \* 7-1 ) mod 26 a+b mod n =0 a\*b mod n=1

=((25+24) \* 15 ) mod 26 = 7--- h

ZEBBW---hello

Polyalphabetic cipher -- one to one

Monoalphabetic cipher—one to many –Playfair cipher, DES,AES…

1.Prime numbers--- Miller – Rabin alg.

2. Fermat’s Theorem

First version: if **P** is a prime and **a** is an integer such that **P** does not divide **a**, then **ap-1 ≡ 1 mod p**

Second version: If P is prime and **a** is an integer, then **ap ≡ a mod p**