```
rsa_encryption.m  rsa_decryption.m  Call_rsa.m  Call_rsa.m  ezpowermod.m  multiply_array_mod.m                                X
 1
 2 e = 11;
 3 n = 899;
 4
 5 F = factor(899);
 6
 7 m = lcm(F(1)-1,F(2)-1);
 8
 9 d = find_inverse_mod(11,m);
10
11 A = 'abcdefghijklmnopqrstuvwxyz# ';
12
13
14 % A
15 M = [605 858 738 01 723 738 173 516 138 296 738 173 468 738 173 01 443 173 01];
16
17 % B
18 %M = [138 173 858 108 296 738 173 468 01 07 380];
19
20 % C
21 %M = [723 108 338 338 749 173 138 173 468 138 723 723 738 469 173 723 108 173 468 229 44 380 173 44 858 01 723 723];
22
23 % D
24 % M = [749 108 229 173 468 138 723 723 738 469 173 7 380 738 173 605];
25
26 % E
27 %M = [07 380 738 173 706 738 338 443 738 858 173 138 723 173 1 173 443 108 338 468 01 858 173 426 380 1 7];
28
29 % F
30 %M = [138 07 173 138 723];
31
32 % G
33 %M = [7 380 1 443 706 173 749 108 229];
34
35 % H
36 H  = [ 8 1 22 5 28 1 7 18 5 1 20 28 19 21 13 13 5 18 ];
37
38 % I
39 I = [8 5 12 12 15 28 23 15 18 12 4];
40
41 % J
42 J = [1 2 19 20 18 1 3 20 28 1 28 9 19 28 3 15 15 12];
43
44 for m = 1:length(M)
45     B(m) = ezpowermod(M(m),d,n);
46     end
47
rsa_decryption.m                                                    40,0-1        Top
"rsa_decryption.m" 51L, 885C written
```

n = 899

e = 11

+5 points on midterm

decode M

Normal Subgroups (discovered by Galois)

Coset Reminder: For $a \in G$, $H \leq G$, $aH = \{ah \mid h \in H\}$. (left coset)

(these are subsets of G, only H will be a subgroup) $Ha = \{ha \mid h \in H\}$. (right coset)

Ex ① $\mathbb{Z}_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$

$H = \langle 3 \rangle = \{3,6,9,0\}$

$1H = 1+H = \{4,7,10,1\}$ ($1+3$, $1+3$)

$H1 =$ same ↑ b/c addition is commutative

Ex ② $G = S_3 = \{(1), (12), (13), (23), (123), (132)\}$

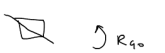
$H = \{(1), (12)\}$

$(123)H = \{(123)(1), (123)(12)\} = \{(123), (13)\}$

$H(123) = \{(1)(123), (12)(123)\} = \{(123), (23)\}$ — not the same

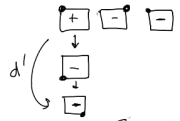
Def'n For subgroup $H \leq G$, we say H is normal if $aH = Ha$ $\forall a \in G$. we denote this by $H \trianglelefteq G$

Ex. In Ex ② above H is not normal.



Ex ③ $D_4 = \{r_0, r_{90}, r_{180}, r_{270}, h, v, d, d'\}$

$K = \{r_0, v, h, r_{180}\}$ (subgroup)



If we pick any $g \in K$ $gK = K$.

eg $vK = \{vr_0, vv, vh, vr_{180}\} = \{v, r_0, r_{180}, h\} = K$

$r_{90}K = \{r_{90}r_0, r_{90}v, r_{90}h, r_{90}r_{180}\} = \{r_{90}, d, d', r_{270}\}$

$Kr_{90} = \{$same, vr_{90}, hr_{90}, same$\} = \{r_{90}, d', d, r_{270}\}$ same

left coset of K = right coset of K for:

$\{r_{90}, r_0, v, h, r_{180}, r_{270}, d, d'\}$

$vK = K = Kv$

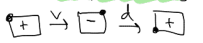
coset is invariant under representative

$r_{90}K = r_{270}K$

remains to show $dK = Kd$

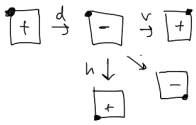
$\{d, dv, dh, dr_{180}\}$

$\{d, r_{90}, r_{270}, d'\}$



$Kd = \{d, vd, hd, r_{180}d\}$

$\{d, r_{270}, r_{90}, d'\}$



$dK = Kd$

so $d'K = Kd'$ (by coset invariance of representative)

Idea: The coset (the subset of elements) is the same if we represent it by any element in the coset.

For our ex: $K = \{r_0, v, h, r_{180}\}$

$K = r_0K = vK = hK = r_{180}K$

$v; r_0, r_{180}, h$

$\{hr_0, hv, hh, hr_{180}\}$

h, r_{180}, r_0, v

$\Rightarrow K \trianglelefteq D_4$

When to tell if a subgroup is normal?

Thm: Given $H \leq G$, then

$$H \trianglelefteq G \iff xHx^{-1} \subseteq H \quad \forall x \in G$$

proof:

($\Rightarrow$) If $H \trianglelefteq G$ then by def'n $xH = Hx \ \forall x \in G$

so given $x \in G$ & $h \in H$ there exist $h' \in H$ s.t. (two things)

$$xh = h'x.$$

now just hit w/ x^{-1}

$$xhx^{-1} = h' \quad \text{this means}$$

anything in $xHx^{-1} \subseteq H$.

($\Leftarrow$) Assume $xHx^{-1} \subseteq H$ show $xH = Hx$

$\forall x \in G$

By assumption, given $x \in G$, $h \in H$ $\exists$ h' s.t.

$$xhx^{-1} = h'$$

(x on left, x on right)

Now mult by x on right

$$\Longrightarrow \quad xh = h'x$$

$$\boxed{xH \subseteq Hx}$$

similarly:

mult on left by x^{-1}

$$hx^{-1} = x^{-1}h'.$$

recall $x \in G$ is arbitrary

so applies to even (x^{-1})

$$h(x^{-1})^{-1} = (x^{-1})^{-1}h'$$

$$hx = xh'$$

h arbitrary

$$\boxed{Hx \subseteq xH}$$

$$xH = Hx$$

$$\boxed{H \trianglelefteq G}$$