Cryptography HW7 0716074 蔡育呈

#1 $n = p \cdot q$

$2881 = 43 \times 67$ let $p = 43, q = 67$ $\phi(n) = (p-1)(q-1) = 42 \cdot 66 = 2772$

$2772 = 42 \times 65 + 42$
$65 = 42 \times 1 + 23$
$42 = 23 \times 1 + 19$
$23 = 19 \times 1 + 4$
$19 = 4 \times 4 + 3$
$4 = 3 \times 1 + 1$

$1 = 4 - 3$
$= 5 \times 4 - 19$
$= 5 \times 23 - 6 \times 19$
$= 11 \times 23 - 6 \times 42$
$= 11 \times 65 - 17 \times 42$
$= 714 \times 65 - 17 \times 2772$

Hence, $65^{-1} \bmod \phi(n) = 714$
$\Rightarrow$ private key $= \{714, 2881\}$ #

#2 let $Y = C \cdot 2^e \bmod n \xrightarrow{\text{Decrypt}} Z = Y^d \bmod n = C^d \cdot 2^{ed} \bmod n$

$= p^{ed} \cdot 2^{ed} \bmod n = 2p \bmod n$

Hence, plaintext $p = Z \cdot 2^{-1} \bmod n$,

we attack the encryption method with a chosen ciphertext attack (Not secure) #

#3. $6^{472} \bmod 3415$

use square and multiply $c = 0,\ f = 1$

for $i = k$ to 0
do $c \leftarrow 2c$
$f \leftarrow f^2 \bmod n$
If $b_i = 1$
then $c \leftarrow c + 1$
$f \leftarrow f \times a \bmod n$

i	11	10	9	8	7	6	5	4	3	2	1	0
bi	0	0	0	1	1	1	0	1	1	0	0	0
c	0	0	0	1	3	7	14	29	59	118	236	472
f	1	1	1	$\xrightarrow{\times a}$ 6	216	3321	2006	166	1416	451	1916	3346

#4 $Z = r^e \bmod n$
$X = ZC \bmod n$
$t = r^{-1} \bmod n$

Decrypt X: $Y = X^d \bmod n = Z^d C^d \bmod n = r^{ed} p^{ed} \bmod n = r \cdot p \bmod n$
eliminate r: $r^{-1} Y = r^{-1} \cdot r \cdot p \bmod n = tY = p \bmod n = p$ #

$0 \le p \le n-1$