Problem 1

(a) $x=5, y=25$ $\quad \gcd(5,25)=5$, so $x^{-1} \bmod y$ does not exist.

$25=5(5)$

(b) $x=12, y=29$ $\quad \gcd(12,29)=1$, so x^{-1} exist

$29=12(2)+5$

$12=5(2)+2$

$5=2(2)+1$

$1=5+2(-2)$

$1=5+(12+5(-2))(-2)$

$1=5(5)+12(-2)$

$1=(29+12(-2))(5)+12(-2)$

$1=29(5)+12(-12)$.

$x^{-1}=17$

(c) $x=24, y=35$ $\quad \gcd(24.35)=1$, so x^{-1} exsit.

$35=24(1)+11$

$24=11(2)+2$

$11=2(5)+1$

$1=11+2(-5)$

$1=11+(24+11(-2))(-5)$

$1=11(11)+24(-5)$

$1=(35+24(-1))(11)+24(-5)$

$1=35(11)+24(-16)$

$x^{-1}=19$

(d) $x=17, y=101$

$\gcd(17,101)=1$, so x^{-1} exsit.

$101=17(5)+16$

$17=16(1)+1$

$1=17+16(-1)$

$1=17+(101+17(-5))(-1)$

$=17(6)+101(-1)$

$x^{-1}=6$

(f) $x=87, y=102$

$\gcd(87,102)=3$, so x^{-1} does not exsit.

$102=87(1)+15$

$87=15(5)+12$

$15=12(1)+3$

$12=3(4)+0$

Scanned with CamScanner

Problem 2, $K=(11,14)$ is a key in an affine cipher over $\mathbb{Z}_{37}$.

(a)

for encrypt: $y = e_K(x) = (ax+b) \bmod 37 = (11x+14) \bmod 37$

for decrypt: $x = d_K(y) = a^{-1}(y-b) \bmod 37$

$\gcd(11,37)=1$

$37 = 11(3)+4$

$11 = 4(2)+3$

$4 = 3(1)+1$

$1 = 4+3(-1)$

$= 4+(11+4(-2))(-1)$

$= 4(3)+11(-1)$

$= (37+11(-3))(3)+11(-1)$

$= 37(3)+11(-10)$

$a^{-1}=27$

$\Rightarrow x = d_K(y) = 27(y-14) \bmod 37. = (27y-378) \bmod 37$

(b)

$d_K(e_K(x)) = d_K[(11x+14) \bmod 37]$

$= 27[(11x+14) \bmod 37] - 378 \pmod{37}$

$= 297x + 378 - 378 \pmod{37}$

$\equiv x \pmod{37}$

Problem 3.

CipherText = "BEEAKFYDJXUQYHYJIQRYHTYJIQDUYJIIKFUHCQ

Since it is encrypted by Shift Cipher, so there are 26 possibilities.

as listed in the following pic.

Scanned with CamScanner

```
t_repo_yuanjieyue/assignment_2/src (master)
$ ./problem3
The 0 possible plaintext:
BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD
The 1 possible plaintext:
CFFBLGZEKYVRZIZKJRSZIUZKJRGCREVZKJJLGVIDRE
The 2 possible plaintext:
DGGCMHAFLZWSAJALKSTAJVALKSHDSFWALKKMHWJESF
The 3 possible plaintext:
EHHDNIBGMAXTBKBMLTUBKWBMLTIETGXBMLLNIXKFTG
The 4 possible plaintext:
FIIEOJCHNBYUCLCNMUVCLXCNMUJFUHYCNMMOJYLGUH
The 5 possible plaintext:
GJJFPKDIOCZVDMDONVWDMYDONVKGVIZDONNPKZMHVI
The 6 possible plaintext:
HKKGQLEJPDAWENEPOWXENZEPOWLHWJAEPOOQLANIWJ
The 7 possible plaintext:
ILLHRMFKQEBXFOFQPXYFOAFQPXMIXKBFQPPRMBOJXK
The 8 possible plaintext:
JMMISNGLRFCYGPGRQYZGPBGRQYNJYLCGRQQSNCPKYL
The 9 possible plaintext:
KNNJTOHMSGDZHQHSRZAHQCHSRZOKZMDHSRRTODQLZM
The 10 possible plaintext:
LOOKUPINTHEAIRITSABIRDITSAPLANEITSSUPERMAN
The 11 possible plaintext:
MPPLVQJOUIFBJSJUTBCJSEJUTBQMBOFJUTTVQFSNBO
The 12 possible plaintext:
NQQMWRKPVJGCKTKVUCDKTFKVUCRNCPGKVUUWRGTOCP
The 13 possible plaintext:
ORRNXSLQWKHDLULWVDELUGLWVDSODQHLWVVXSHUPDQ
The 14 possible plaintext:
PSSOYTMRXLIEMVMXWEFMVHMXWETPERIMXWWYTIVQER
The 15 possible plaintext:
QTTPZUNSYMJFNWNYXFGNWINYXFUQFSJNYXXZUJWRFS
The 16 possible plaintext:
RUUQAVOTZNKGOXOZYGHOXJOZYGVRGTKOZYYAVKXSGT
The 17 possible plaintext:
SVVRBWPUAOLHPYPAZHIPYKPAZHWSHULPAZZBWLYTHU
The 18 possible plaintext:
TWWSCXQVBPMIQZQBAIJQZLQBAIXTIVMQBAACXMZUIV
The 19 possible plaintext:
UXXTDYRWCQNJRARCBJKRAMRCBJYUJWNRCBBDYNAVJW
The 20 possible plaintext:
VYYUEZSXDROKSBSDCKLSBNSDCKZVKXOSDCCEZOBWKX
The 21 possible plaintext:
WZZVFATYESPLTCTEDLMTCOTEDLAWLYPTEDDFAPCXLY
The 22 possible plaintext:
XAAWGBUZFTQMUDUFEMNUDPUFEMBXMZQUFEEGBQDYMZ
The 23 possible plaintext:
YBBXHCVAGURNVEVGFNOVEQVGFNCYNARVGFFHCREZNA
The 24 possible plaintext:
ZCCYIDWBHVSOWFWHGOPWFRWHGODZOBSWHGGIDSFAOB
The 25 possible plaintext:
ADDZJEXCIWTPXGXIHPQXGSXIHPEAPCTXIHHJETGBPC
```

Problem 4.

As we kow,

for encrypt : $y = e_K(x) = (x+K) \bmod 26$

for decrypt : $x = d_K(y) = (y-K) \bmod 26$

Since K is involutory key, $e_K(x) = d_K(y)$

we have
$$
\begin{aligned}
x &= d_K(e_K(x)) \\
&= e_K(e_K(x)) \\
&= e_K[(x+K) \bmod 26] \\
&= [(x+K) \bmod 26 + K] \bmod 26 \\
&= (x+2K) \bmod 26.
\end{aligned}
$$

Now we need $2k \bmod 26 = 0$, then k has two options.

one is $K=0$, the other is $k=13$.

Problem 5.

Given an ciphertext = "tcabtiqmfheqqmrmvmtmaq" using Affine cipher, and $a=3$, and Z_{26}.

Since $a=3$, from extended eucliblean algorithm, we could get $a^{-1}=9$.

$$
\begin{aligned}
&\gcd(3,26)=1 & 1 &= 3+2(-1) \\
&26 = 3(8)+2 & &= 3+(26+3(-8))(-1) \\
&3 = 2(1)+1 & &= 26(-1)+3(9) \\
& & a^{-1} &= 9.
\end{aligned}
$$

then for the K (a,b), we could try b in the range [0, 25] to find the 26 possibilites, and pick up the meaningful one from them.

from the pic listed below, the 14th possibility is meaningful when b=14,

the plaintext should be "twentysixpossibitities".

```
$ ./problem5
The 0 possibility is:
psajpuoetlkooexehepeao
The 1 possibility is:
gjraglfvkcbffvovyvgvrf
The 2 possibility is:
xairxcwmbtswwmfmpmxmiw
The 3 possibility is:
orziotndskjnndwdgdodzn
The 4 possibility is:
fiqzfkeujbaeeunuxufuqe
The 5 possibility is:
wzhqwbvlasrvvlelolwlhv
The 6 possibility is:
nqyhnsmcrjimmcvcfcncym
The 7 possibility is:
ehpyejdtiazddtmtwtetpd
The 8 possibility is:
vygpvaukzrquukdknkvkgu
The 9 possibility is:
mpxgmrlbqihllbubebmbxl
The 10 possibility is:
dgoxdicshzyccslsvsdsoc
The 11 possibility is:
uxfouztjyqpttjcjmjujft
The 12 possibility is:
lowflqkaphgkkatadalawk
The 13 possibility is:
cfnwchbrgyxbbrkrurcrnb
The 14 possibility is:
twentysixpossibilities
The 15 possibility is:
knvekpjzogfjjzszczkzvj
The 16 possibility is:
bemvbgaqfxwaaqjqtqbqma
The 17 possibility is:
svdmsxrhwonrrhahkhshdr
The 18 possibility is:
jmudjoiynfeiiyrybyjyui
The 19 possibility is:
adluafzpewvzzpipspaplz
The 20 possibility is:
ruclrwqgvnmqqgzgjgrgcq
The 21 possibility is:
iltcinhxmedhhxqxaxixth
The 22 possibility is:
zcktzeyodvuyyohorozoky
The 23 possibility is:
qtbkqvpfumlppfyfifqfbp
The 24 possibility is:
hksbhmgwldcggwpwzwhwsg
The 25 possibility is:
ybjsydxncutxxngnqnynjx
```

Problem 6.

Given

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

, π is permutation of $\{1, \ldots, 8\}$.

ⓐ Compute the permutation π^{-1}; we could get the π^{-1} by sorting the $\pi(x)$ in to ascending order.

x	1	2	3	4	5	6	7	8
$\pi^{-1}(x)$	2	4	6	1	8	3	5	7

ⓑ Decrypt the ciphertext $m = 8$, using key π.

12345678 12345678 12345678 12345678

"TGEEMNEL|NNTDROEO|AAHDOETC|SHAEIRLM"

"GENTLEME|NDONOTRE|ADEACHOT|HERSMAIL"

first, we split the ciphertext into part, every parts has a length m.
then, inside a part, we use π^{-1} table to rearrange the character,
finally, we could get the plaintext.

Problem 7.

for classical cryptosystem, every user need to have $m-1$ unqiue keys to commute with the other $m-1$ users. And Because two users communicate with each other could share a pair key, so the total num of key need to be generated is $\frac{m(m-1)}{2}$, if $m = 500$, the $\frac{m(m-1)}{2} = \frac{500(500-1)}{2} = 124750$.

while for public key cryptosystem, every users got a pair of public and private key, if only they could keep their private key confidential, every user has 2 keys is enough to communicate with the other $(m-1)$ users. So total keys needed to be generated is $2m$. if $m=500$, then total keys is 1000.

Problem 8.

given n, e, d, ask to factor n

$$n = p * q$$

$$\varphi(n) = (p-1) * (q-1)$$

$$= pq - p - q + 1 = n - p - \frac{n}{p} + 1$$

$$p\varphi(n) = pn - p^2 - n + p$$

$$\Rightarrow \quad p^2 + (\varphi(n) - n - 1)p + n = 0.$$

$a = 1$

$b = \varphi(n) - n - 1$

$c = n$

according to the quadratic formular.

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$= -\frac{\varphi(n) - n - 1}{2} \pm \sqrt{\left(\frac{\varphi(n) - n - 1}{2}\right)^2 - n}$$

x has two values, one is p, the other is q.

and we know $ed \equiv 1 \mod (\varphi(n))$. so $\varphi(n) = \frac{1}{m} * (ed - 1)$

$m \in [1 \dots)$

so in the c program, we simulate this process.

Scanned with CamScanner

Problem 9.

If the attacker choose a ciphertext $\hat{y}$ as the multiplicative inverse of the ciphertext y, then $y \cdot \hat{y} = 1 \Rightarrow e_K(x) \cdot e_K(\hat{x}) \pmod{n} = 1$.

We know that if $\gcd(\hat{y}, n) = 1$, then such $\hat{y}$ exist,

and due to the multiplicative property:

$$y \cdot \hat{y} = e_K(x) \cdot e_K(\hat{x}) \pmod{n}$$
$$= e_K(x \cdot \hat{x} \pmod{n}) = 1.$$

Since RSA encryption, $e_K(x) = x^b \pmod{n}$, from the equation above

$(x \cdot \hat{x})^b \equiv 1 \pmod{n} \Rightarrow (x \cdot \hat{x}) \equiv 1 \pmod{n}$

Because we know that n is the product of two primes,

for $\gcd(\hat{x}, n)$, it has two cases:

① $\gcd(\hat{x}, n) = \hat{x}$ ($\hat{x}$ is a factor of n)

now $\hat{x}$ is one of p or q. thus, we could factor n, then find x.

② $\gcd(\hat{x}, n) = 1$ ($\hat{x}$ and n are co primes)

in this case $\hat{x}^{-1}$ exist, and $\hat{x}^{-1} \pmod{n} = x$.

So from above, we know that RSA is insecure against chosen ciphertext a[ttack]

Problem 10.

(a). if $p = 2$, $q = 13$

then $n = p * q = 26$

$\varphi(n) = (p-1) * (q-1) = 13$

$$\begin{cases} \gcd(e, n) = 1 \\ \gcd(e, \varphi(n)) = 1 \end{cases}$$

$\Rightarrow e =$ all primes that are co primes to n and $\varphi(n)$ at the same time

if $p = 13$, $q = 17$

then $n = p * q = 221$

$\varphi(n) = (p-1) * (q-1) = 192$

$$\begin{cases} \gcd(e, n) = 1 \\ \gcd(e, \varphi(n)) = 1 \end{cases}$$

$\Rightarrow e =$ all primes that are co primes to n and $\varphi(n)$ at the same time.

(b) from the defininition, we would get the equation below.

$y_1 = ex + e$ ⇐ Affine phase

$y_2 = (y_1)^e$ ← modular exponentiation phase.

$= (ex+e)^e$

$= e^e \cdot x^e + e^e$

so it is actually kind of the same as RSA.

it is a well defined cryptosystem to this term.

(c) As discussed above, it's similar to RSA. that it is secure.

while it's insecure to ciphertext attack, just the same as RSA.

Scanned with CamScanner