Math 445
Introduction to Cryptography
Homework Solutions
January 26, 2004

2.13.2 Using the standard encoding of a-z as 0-25, *howareyou* becomes
8 14 22 0 17 4 24 14 20
Applying the affine transformation $x \mapsto 5x + 7 \pmod{26}$ yields:
$7 \mapsto 42 \equiv 16 \pmod{26}$
$14 \mapsto 77 \equiv 25 \pmod{26}$
$22 \mapsto 117 \equiv 13 \pmod{26}$
$0 \mapsto 7 \pmod{26}$
$17 \mapsto 92 \equiv 14 \pmod{26}$
$4 \mapsto 27 \equiv 1 \pmod{26}$
$24 \mapsto 127 \equiv 23 \pmod{26}$
$14 \mapsto 77 \equiv 25 \pmod{26}$
$20 \mapsto 107 \equiv 3 \pmod{26}$

Translating back to letters gives the ciphertext: *QZNHOBXZD*. The decryption function is $y \mapsto a'x + b'$ where $5a' \equiv 1 \pmod{26}$ and $b' = -7a' \pmod{26}$. Brute force (or more sophisticated methods ....) reveals that $a' = 21$ and then $b' = 9$. Straightforward calculation shows that it works, i.e., it transforms the ciphertext back into the plaintext.

2.13.4 Since C (2) decrypts to h (7) and R (17) decrypts to a (0), the decryption function $y \mapsto a'y + b'$ satisfies the equations

$$\begin{aligned} 7 &\equiv 2a' + b' \pmod{26} \\ 0 &\equiv 17a' + b' \pmod{26}. \end{aligned}$$

The second equation gives $b' \equiv -17a' \equiv 9a' \pmod{26}$. Substituting into the first equation then implies that $7 \equiv 11a' \pmod{26}$. Since $19 \cdot 11 \equiv 1 \pmod{26}$, we have $a' \equiv 19 \cdot 7 \equiv 3 \pmod{26}$ and $b' \equiv 9 \cdot 3 \equiv 1 \pmod{26}$. Thus the decryption function is $y \mapsto 3y + 1 \pmod{26}$ and the message decrypts to *happy*.

2.13.5 There is no advantage because the composition of two affine ciphers is another affine cipher. Indeed, if we compose $y = ax + b$ with $z = cy + d$, we get

$$z = cy + d = c(ax + b) + d = (ac)x + (bc + d).$$

which is just an affince cipher with key $(ac, bc + d)$.

2.13.6 If we work modulo 27, then the legitimate keys are (a, b) where the greatest common divisor (gcd) of a and 27 is 1 and b is arbitrary. Since $27 = 3^3$, $\gcd(a, 27) = 1$ if and only if 3 does not divide a. Moreover, if $a' \equiv a \pmod{27}$ and $b' \equiv b \pmod{27}$ then (a, b) and (a', b') give the same encryption function. In other words, we should regard a and b as numbers modulo 27. So we get every key exactly once if we choose a from the set $\{1, 2, 4, 5, 7, 8, \ldots, 25, 26\}$ and b from the set $\{0, 1, 2, \ldots, 25, 26\}$. There are 18 choices for a and 27 choices for b, so 486 keys in all.
Working modulo 29 the story is similar, except that 29 is prime, so $\gcd(a, 29) = 1$ for any a not divisible by 29. Thus we have 28 choices for a and 29 choices for b and so 812 keys in all.

2.13.7 Suppose that $\gcd(\alpha, 26) = d > 1$. Then d divides 26 and so $(26/d)$ is an integer. Let x_2 be any integer modulo 26 and set $x_1 = x_2 + (26/d)$. Since $d > 1$, we have $0 < (26/d) < 26$ and so $x_1 \not\equiv x_2 \pmod{26}$. Now we calculate the encryption of x_1:

$$\begin{aligned} \alpha x_1 + \beta &= \alpha(x_2 + (26/d)) + \beta \\ &= \alpha x_2 + \beta + \alpha(26/d). \end{aligned}$$

But $\alpha(26/d) = (\alpha/d)26$ and since d divides α, the quantity $(\alpha/d)26$ is an integer times 26. Thus the calculation above shows that

$$\alpha x_1 + \beta \equiv \alpha x_2 + \beta \pmod{26}.$$

This means two different plaintext characters (namely x_1 and x_2) encrypt to the same ciphertext character and so we will not be able to decrypt.

2.14.2 Using Mathematica:

The ciphertext is stored in `lcll`:

```
In[105] := lcll
Out[105] = lcllewljazlnnzmvyiylhrmhza
```

Do a frequency count:

```
In[106] := frequency[lcll]
Out[106] =
```

$$\{\{a,2\},\{b,0\},\{c,1\},\{d,0\},\{e,1\},\{f,0\},\{g,0\},\{h,2\},\{i,1\},$$

$$\{j,1\},\{k,0\},\{l,6\},\{m,2\},\{n,2\},\{o,0\},\{p,0\},\{q,0\},\{r,1\},$$

$$\{s,0\},\{t,0\},\{u,0\},\{v,1\},\{w,1\},\{x,0\},\{y,2\},\{z,3\}\}$$

The most common letter is l so we guess this is a shift by 7. Try it out:

```
In[107] := affinecrypt[lcll,1,-7]
Out[107] = eveexpectseggsforbreakfast
```

2.14.3 This is like problem 13.4: we need to solve

$$8 \equiv 4a' + b' \pmod{26}$$
$$5 \equiv 3a' + b' \pmod{26}$$

Subtracting the second equation from the first gives

$$3 \equiv a' \pmod{26}$$

and substituting into either equation gives

$$22 \equiv b' \pmod{26}.$$

Now use Mathematica to do the decryption:

```
In[108] := edsg
Out[108] = edsgickxhuklzveqzvkxwkzukcvuh

In[109] := affinecrypt[edsg,3,22]
Out[109] = ifyoucanreadthisthankateacher
```