TMA4155 Cryptography, introduction 2010–12–01

Suggested solution

Problem 1

Your public key is $X = 2^9 \bmod 101 = 512 \bmod 101 = 7$ (since $512 = 5 \cdot 101 + 7$).

Your shared secret with Alice is $g^{ax} \bmod 101 = A^x \bmod 101$. We compute this efficiently as follows:

$$A^x = 34^9 = (34^3)^3$$
$$34^3 \bmod 101 = 39304 \bmod 101 = 15$$
$$A^x \bmod 101 = 15^3 \bmod 101 = 3375 \bmod 101 = 42,$$

so the shared secret is 42.

Problem 2

a. Below, I use the notation $2_{\mathtt{B}}$ for the number 2 associated with the ciphertext letter `B`, and $8_{\mathtt{i}}$ for the number 8 associated with the ciphertext letter `i`, etc.

The affine cipher is given by $c_i = ax_i + b \bmod 26$, where x_i is the code of plaintext letter number i, and c_i is the code of the corresponding ciphertext letter. From the fact that `ican` is encrypted as `BZHU`, we get the four equations

$$8_{\mathtt{i}}a + b \equiv 1_{\mathtt{B}} \pmod{26} \qquad 2_{\mathtt{c}}a + b \equiv 25_{\mathtt{Z}} \pmod{26}$$
$$0_{\mathtt{a}}a + b \equiv 7_{\mathtt{H}} \pmod{26} \qquad 13_{\mathtt{n}}a + b \equiv 20_{\mathtt{U}} \pmod{26}$$

from which we immediately get $b = 7$ and

$$8a \equiv 20, \quad 2a \equiv 18, \quad 13a \equiv 13 \pmod{26}.$$

The first two congruences can be divided by 2, and the third by 13, yielding

$$4a \equiv 10, \quad a \equiv 9 \pmod{13},$$
$$a \equiv 1 \pmod{2}.$$

Of these, the first follows from the second since $4 \cdot 9 = 36 \equiv 10 \pmod{26}$, so we only need to solve the second and third together. They have the solution $a = 9$.

Thus the encryption function is $c_i = 9x_i + 7 \bmod 26$. The inverse of 9 modulo 26 is 3, since $3 \cdot 9 = 27 \equiv 1 \pmod{26}$. So multiplying by 3 we get $3c_i \equiv x_i + 21 \pmod{26}$, so that the decryption function is given by

$$x_i = 3c_i + 5 \bmod 26.$$

Upon decryption, the plaintext turns out to be `icanhazsecrets`, or with capitalization and spaces: "I can haz secrets".

b. The key is repeated as often as necessary, then each letter of the key and the corresponding letter of the plaintext are converted to numbers and added modulo 26. Finally the results are converted back to letters and form the ciphertext.

If the ciphertext is $c_1 c_2 \ldots c_n$ then for $\ell = 1, 2, 3, \ldots$ one counts the number of indices i for which $c_i = c_{i+\ell}$. When ℓ is the keylength, or a multiple of the keylength, this coincidence count can be expected to be higher.

c. First, split the given ciphertext in groups equal to the keylength:

YSC ATE JYC WPA NAF JCG XPY XTJ DMP TVC SHG YSQ YLR NDR NNQ

Then perform a frequency count for the second and third place in each group. (There is no need to do so for the first place, since the corresponding letter of the key is already known.) The result can be summarized in the following table.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	1		1	1				1				1	1	1		2			2	2		1			1	
3	1		3		1	1	2			1						1	2	2	1							1	

For position 2, it seems likely that plaintext `e` should correspond to one of `P`, `S` or `T`, which would make the second letter of the key equal to `L`, `O` or `P`. The three choices would make the three letters `PST` decrypt as `ehi`, `aef`, or `zde`. The third seems somewhat less likely than the first two.

For position 3, likely ciphertext choices for plaintext `e` are `C`, `G`, `Q` or `R`, making the second letter of the key equal to `Y`, `C`, `M` or `N`. These four choices make the frequent letters `CGQR` decrypt as `eist`, `aeop`, `puef`, `otde`. Of these the first seems more plausible.

We can also state our findings for likely key letters as the string `F[LOP][YCMN]` where square brackets surround alternatives for the second and third letter. We have some preference for the first letter, and since indeed `FLY` is an actual word, we should let that be our first guess.

In fact, using `FLY` as the key, the ciphertext decodes into

`thevigenerecipheriseasilybrokenwithstatistics`.

Inserting spaces, capitalization and an accent, we end up with the final decryption “The Vigenère cipher is easily broken with statistics”.

Problem 3

We are looking for the factorization in the form $24881 = (x-y)(x+y) = x^2 - y^2$. Writing this as $x^2 - 24881 = y^2$,we expect y to be relatively small, so we start with the smallest $x > \sqrt{24881}$, i.e., $x = 158$: But $158^2 - 24881 = 83$ which is not a square. Next we try $x = 159$, and find $159^2 - 24881 = 400 = 20^2$. So indeed, $24881 = (159-20)(159+20) = 139 \cdot 179$.

This procedure is quite efficient at finding factorizations where the factors are close together. Since the security of RSA is dependent on adversaries being unable to factor the modulus, the two prime factors need to be far apart.

Problem 4

a. The order of x is the smallest number $r \geq 1$ so that $x^r \equiv 1 \pmod{p}$. The order must divide $p-1$. But $p-1 = 2q$ has only the divisors 1, 2, q, $2q$, so those are the only possibilities for the order of x.

x is called a primitive root if its order is $p-1$ (that is, $2q$ in the present setting).

b. We note that $107 = 2 \cdot 53 + 1$ is a safe prime, with corresponding Sophie Germain prime 53.

$2^{34} = 17179869184$ is too large to be handled on a small calculator, but powers just a little smaller can be handled easily. For example, $2^{10} = 1024 = 9 \cdot 107 + 61 \equiv 61 \pmod{107}$, so $2^{20} \equiv 61^2 = 3721 = 34 \cdot 107 + 83 \equiv 83$, and $2^{53} = (2^{20})^2 \cdot 2^{10} \cdot 8 \equiv 83^2 \cdot 61 \cdot 8 = 3361832 = 31419 \cdot 107 - 1 \equiv -1 \pmod{107}$.

Thus $2^2 = 4 \not\equiv 1 \pmod{107}$ and $2^{53} \equiv -1 \not\equiv 1 \pmod{107}$, so the period of 2 is neither 2 nor 53 (and certainly not 1) so it must be 106, so that 2 is indeed a primitive root.

We also find $2^{34} = 2^{20} \cdot 2^{10} \cdot 2^4 \equiv 83 \cdot 61 \cdot 16 = 81008 = 757 \cdot 107 + 9 \equiv 0 \pmod{107}$, in other words $2^{34} \bmod 107 = 9$.

c. It is tempting to just take the square root of $2^{34} \bmod 107 = 9$, but we can only conclude from it that $2^{17} \equiv \pm 3 \pmod{107}$. Computing, we get indeed the opposite sign: $2^{17} \equiv -3 \pmod{107}$. If we multiply by $2^{53} \equiv -1 \pmod{107}$, we obtain $2^{70} \equiv 3 \pmod{107}$.

Now 3 is a quadratic residue modulo 107, so it has period 53. We can see this directly: $3^{53} \equiv (2^{70})^{53} = 2^{70\cdot 53} = 2^{35\cdot 106} = (2^{106})^{35} \equiv 1 \pmod{107}$ by Fermat's little theorem.

d. The map $r \mapsto g^r \bmod p$ is a one-to-one map of $\mathbb{Z}_q$ onto the set Q_p of invertible quadratic residues modulo p. Thus picking r at random from $\mathbb{Z}_q$ amounts to picking g^r at random from Q_p. If we ensure that all possibilities are equally likely, then since $y \mapsto yh^x$ is a one-to-one map of Q_p onto itself, $g^r h^x$ is just as uniformly picked at random no matter what x is. Hence there is no information about x available.

e. From the assumptions we have $4^{22} \cdot 9^{10} \bmod 107 = 47 = 4^8 \cdot 9^{42}$, so that $4^{22-8} \equiv 9^{42-10}$, i.e.,

$$4^{14} \equiv 9^{32} \pmod{107}.$$

Since 4 has period 53, we want to raise this to a power $14^{-1} \bmod 53 = 19$. (We find this by the extended Euclidean algorithm. The answer is easily checked, since $14 \cdot 19 = 266 = 5 \cdot 53 + 1$.) The result is

$$4 \equiv 9^{32\cdot 19} \pmod{107}.$$

Since 9 also has order 53, we simplify this by noting $32 \cdot 19 = 608 = 11 \cdot 53 + 25$, so the general solution to $9^z \equiv 4 \pmod{1)07}$ is given by

$$z \equiv 25 \pmod{53}.$$

We can compare this with the earlier result $4^{70} \equiv 9 \pmod{107}$. Taking the 25th power of this we get

$$9^{25} \equiv 4^{25\cdot 70} \equiv 4^{1750 \bmod 53} = 4$$

since $1750 = 33 * 53 + 1 \equiv 1 \pmod{53}$.

The somewhat trivial lesson from this is that, if two commitments for different messages happen to be the same, then one can solve the equation $h^z \equiv g \pmod{p}$ for z.

A more important lesson comes from the converse: Namely that if z is known then it is easy to create a new message to fit an earlier commitment for another message. Say that Alice has already published a commitment $c = g^r h^x \bmod p$ for some message x. Now she wants to change her mind and claim that c is a commitment for a *different* message x': To be convincing, she needs to come up with some r' so that $c = g^{r'} h^{x'} \bmod p$. For this, she needs to solve the equation $g^{r'} h^{x'} \equiv g^r h^x \pmod{p}$ for r'. If we substitute h^z for g in this equation, it becomes $h^{zr'+x'} \equiv h^{zr+x} \pmod{p}$, which is equivalent to $zr' + x \equiv zr + x \pmod{q}$, which is easily solved for r'.

Therefore, g and h must be chosen so that it is unreasonable even to suspect that Alice knows the solution z to $h^z \equiv g \pmod{p}$. Returning to the first, "somewhat trivial" lesson, we see that, in fact, suspecting Alice of having substituted the message x' for some other message x, is equivalent to suspecting her of knowing (or being able to find) z.