Trondheim, December 12, 2005.

TMA4155 Cryptography, Intro — Solutions

Problem 1

a. A symmetric cryptosystem consists of two algorithms, one for encryption and one for decryption, so we must describe them. We should also specify the set of messages, the set of ciphertexts and the set of keys.

Suppose we have a pseudo-random number generator (PRNG) g that on input of a key k, initialization vector iv and a count n outputs a sequence of numbers $z_1, z_2, \ldots, z_n$, $0 \leq z_i < 26$.

The set of keys for the cryptosystem will be equal to the set of keys for the PRNG. The message set will be the set of strings of letters from the English alphabet. The ciphertext set consist of a string encoding the initialization vector followed by a string of letters from the English alphabet.

The encryption algorithm takes as input a key and a message consisting of n letters. First it converts the message letters into a sequence of numbers $m_1, m_2, \ldots, m_n$, using the correspondence $A \leftrightarrow 0, B \leftrightarrow 1, \ldots, Z \leftrightarrow 25$. Then it samples a random initialization vector iv and computes first $g(k, iv, n) = (z_1, z_2, \ldots, z_n)$, then $c_i = (m_i + z_i) \bmod 26$, $1 \leq i \leq n$. Finally, the sequence $c_1, c_2, \ldots, c_n$ is converted into a string of letters, and the ciphertext is the concatenation of the initialization vector and this string of letters.

The decryption algorithm takes as input a key and a ciphertext. First it splits the ciphertext into two parts, one part encoding the initialization vector iv and one part consisting of a string of n letters. The decryption algorithm converts the second part into a sequence of integers $c_1, c_2, \ldots, c_n$, then computes $g(k, iv, n) = (z_1, z_2, \ldots, z_n)$ and $m_i = (c_i - z_i) \bmod 26$, $1 \leq i \leq n$. The sequence $m_1, m_2, \ldots, m_n$ is converted into a string of letters, and this is the message output.

It is clear that decrypting any encryption of a message will return the original message, since

$$m_i \equiv c_i - z_i \equiv m_i + z_i - z_i \equiv m_i \pmod{26}.$$

There are many other possibilities for constructing a valid cryptosystem, such as variants of *counter mode*, *output feedback mode* and *cipher feedback mode*. Note that such systems may be insecure, even though the PRNG is secure.

b. We first observe that the first 14 letters of both ciphertexts are equal, the first 14 letters encode the initialization vector, therefore the two ciphertexts have been encrypted with the same initialization vector.

Let $z_1, z_2, \ldots, z_{15}$ be the output of the PRNG. If we represent the letters in second part of the ciphertext as the number sequences $c_1, c_2, \ldots, c_{14}$ and

$c'_1, c'_2, \ldots, c'_{15}$, and the message letters as $m_1, m_2, \ldots, m_{14}$ and $m'_1, m'_2, \ldots, m'_{15}$, we know that

$$c_i - c'_i \equiv m_i + z_i - m'_i - z_i \equiv m_i - m'_i \pmod{26},$$

which means that

$$m'_i \equiv m_i + (c'_i - c_i) \pmod{26} \text{ and } m_i \equiv m'_i + (c_i - c'_i) \pmod{26}.$$

First we compute the following table. (Note that everything is done modulo 26, so $(c_i - c'_i) + (c'_i - c_i) = 26$ in the table.)

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
c_i	2	23	23	4	7	16	19	1	4	0	22	0	22	23
c'_i	7	19	9	1	5	0	4	7	1	8	3	22	8	7
$c_i - c'_i$	21	4	14	3	2	16	15	20	3	18	19	4	14	16
$c'_i - c_i$	5	22	12	23	24	10	11	6	23	8	7	22	12	10

If the first message contains the letters AES, then $m_1 = 0$, $m_2 = 4$ and $m_3 = 18$. That would give $m'_1 = 0 + 5 = 5$, $m'_2 = 4 + 22 \bmod 26 = 0$ and $m'_3 = 18 + 12 \bmod 26 = 4$, or the letters FAE. This does not ring any bells.

But if the second message contains the letters AES, then $m'_1 = 0$, $m'_2 = 4$ and $m'_3 = 18$ which gives $m_1 = 21$, $m_2 = 8$ and $m_3 = 14 + 18 \bmod 26 = 6$ and the letters VIG. VIG suggests the word VIGENERE, so we try that.

Then $m_4 = 4$, $m_5 = 13$, $m_6 = 4$, $m_7 = 17$ and $m_8 = 4$. From this we get that $m'_4 = 4 + 23 \bmod 26 = 1$, $m'_5 = 13 + 24 \bmod 26 = 11$, $m'_6 = 4 + 10 = 14$, $m'_7 = 17 + 11 \bmod 26 = 2$, $m'_8 = 4 + 6 = 10$ and the letters BLOCK. We are clearly on the right track, with the first message starting with VIGENERE and the second starting with AESBLOCK.

Remember that AES is a block *cipher*. We guess CIPHER for the second message and get $m'_9 = 2$, $m'_{10} = 8$, $m'_{11} = 15$, $m'_{12} = 7$, $m'_{13} = 4$ and $m'_{14} = 17$. This gives us $m_9 = 2+3 = 5$, $m_{10} = 8+18 \bmod 26 = 0$, $m_{11} = 15+19 \bmod 26 = 8$, $m_{12} = 7+4 = 11$, $m_{13} = 4+14 = 18$ and $m_{14} = 17+16 \bmod 26 = 7$ and the letters FAILSH.

Unfortunately there was an error in both ciphertexts, in that they contained one letter too much. So the first ciphertext decrypts to VIGENEREFAILS, while the second decrypts to AESBLOCKCIPHER.

The discussion above clearly shows that we can tell which message belongs to which ciphertext, even if we could not recover the entire ciphertext. This is in contrast to binary messages, where it is impossible to tell which message belongs to which ciphertext.

c. The birthday paradox suggests that when sampling random elements from a set with n elements, it is likely that we will see a duplicate before we have sampled roughly $\sqrt{n}$ elements.

Our set has size 26^{14}, which means that is is likely that we will see a duplicate before we have sampled roughly $26^7 \approx 8 \cdot 10^9$ elements.

Problem 2

a. The order of a number g modulo p means the smallest integer $i \geq 1$ such that $g^i \equiv 1 \pmod{p}$.

Note that 23 is prime, as is 47. We know that the order divides $p-1$, so $g = 2$ has either order 1, 2, 23 or 46. It is obvious that 2 does not have order 1, so all we need to show is that $g^{23} \equiv 1 \pmod{47}$.

An easy computation shows that $2^{23} - 1 = 8388608 - 1 = 178481 \cdot 47$.

b. First we interpret the key as $(p, q, g, x) = (47, 23, 2, 7)$, and the signatures as $(m_1, (r_1, s_1)) = (13, (13, 14))$ and $(m_2, (r_2, s_2)) = (12, (13, 14))$.

We first find an inverse of 14 modulo 23 using the extended Euclidian algorithm:

$$\begin{aligned} 23 &= 1 \cdot 14 + 9 & &= 2 \cdot 14 - 3 \cdot 23 + 3 \cdot 14 = 5 \cdot 14 - 3 \cdot 23 \\ 14 &= 1 \cdot 9 + 5 & &= 2 \cdot 14 - 3 \cdot 9 \\ 9 &= 1 \cdot 5 + 4 & &= 5 - 9 + 5 = 2 \cdot 5 - 9 \\ 5 &= 1 \cdot 4 + 1 & 1 &= 5 - 4 \end{aligned}$$

An inverse of 14 is 5. Then we compute:

$$\begin{aligned} u_1 &= 5 \cdot 13 \bmod 23 = 19 & \qquad v_1 &= 5 \cdot 13 = 19 \\ u_2 &= 5 \cdot 12 \bmod 23 = 14 & \qquad v_2 &= 5 \cdot 13 = 19 \end{aligned}$$

And we compute

$$2^{19}7^{19} \equiv 3 \cdot 7^{11} \cdot 7^8 \equiv 3 \cdot 36 \cdot 16 \equiv 36 \pmod{47}.$$

Since $36 \equiv 13 \pmod{23}$, the first message-signature pair is valid.

Next we compute

$$2^1 47^1 9 \equiv 28 \cdot 36 \cdot 16 \equiv 7 \pmod{47}.$$

Since $7 \not\equiv 13 \pmod{23}$, the second message-signature pair is invalid.

c. Since 2 has order 23 and $\sqrt{23} \approx 5$, we compute the following table:

i	0	1	2	3	4
$2^i \bmod 47$	1	2	4	8	16

We want to multiply by $2^{-5} \bmod 47$, so we need an inverse of 32 modulo 47. We compute:

$$\begin{aligned} 47 &= 32 + 15 & &= 15 \cdot 47 - 22 \cdot 32 \\ 32 &= 2 \cdot 15 + 2 & &= 15 - 7 \cdot 32 + 14 \cdot 15 = 15 \cdot 15 - 7 \cdot 32 \\ 15 &= 7 \cdot 2 + 1 & 1 &= 15 - 7 \cdot 2 \end{aligned}$$

We take the inverse 25 (which is congruent to -22 modulo 47).

Now we compute $25 \cdot 7 \equiv 34 \pmod{47}$, $25 \cdot 34 \equiv 4 \pmod{47}$, so

$$2^2 \equiv 2^{-5} \cdot 2^{-5} \cdot 7 \pmod{47},$$

or

$$7 \equiv 2^1 2 \pmod{47}.$$

d. First we compute $r \equiv 2^9 \equiv 42 \pmod{47}$, and $42 \equiv 19 \pmod{23}$. Then we need an inverse of 19 modulo 23:

$$\begin{aligned} 23 &= 1 \cdot 9 + 5 & &= 2 \cdot 23 - 4 \cdot 9 - 9 = 2 \cdot 23 - 5 \cdot 9 \\ 9 &= 5 + 4 & &= 5 - 9 + 5 = 2 \cdot 5 - 9 \\ 5 &= 4 + 1 & 1 &= 5 - 4 \end{aligned}$$

We take the inverse 18 (which is congruent to -5 modulo 23) and compute

$$s \equiv 18(11 + 12 \cdot 19) \equiv 4302 \equiv 1 \pmod{23}.$$

Problem 3

a. We have that $p - 1 = 18 = 2 \cdot 3^2$ and $q - 1 = 22 = 2 \cdot 11$, so we choose $e = 5$ and compute an inverse of 5 modulo 396:

$$396 = 79 \cdot 5 + 1 \qquad 1 = 396 - 79 \cdot 5.$$

We take $d = 317$ which is congruent to -79 modulo 396.

The public key is $(437, 5)$, the private key is $(437, 317)$.

b. A signature scheme consists of three algorithms, a key generation algorithm, a signing algorithm and a verification algorithm.

The key generation algorithm first chooses two random primes p and q (for instance by repeatedly choosing random numbers and checking if they are prime with the Rabin-Miller test). Then it finds some number e that is relatively prime to $(p-1)(q-1)$ and computes an inverse d of e modulo $(p-1)(q-1)$. It then outputs the public key (n, e) and the secret key (n, d), where $n = pq$.

The signing algorithm takes as input a secret key (n, d) and a message $m \in \{0, 1, \ldots, n-1\}$. It computes $s = m^d \bmod n$ and outputs the tag s.

The verification algorithm takes as input a public key (n, e), a message m and a tag s from $\{0, 1, \ldots, n-1\}$. It computes $m' = s^e \bmod n$. If $m = m'$, it outputs VALID, otherwise INVALID.

To construct a valid message-signature pair for the given public key, we can either explain how we would factor the modulus, compute the secret exponent and then use the signing algorithm. Or we can observe that any pair ($s^e \bmod 1000216006039, s$) will be a valid message-signature pair, specifically will $(32, 2)$ be a valid pair.

c. We compute that

$$555 \cdot 835472 = 59 \cdot 7859101 + 1$$

so the two numbers are inverses. Now we note that

$$(m^{-1})^d \equiv m^{-d} \equiv (m^d)^{-1} \equiv s^{-1} \pmod{n}.$$

Since the two messages are inverses, the two signatures will also be inverses modulo 7859101. We compute an inverse:

$$\begin{aligned}
7859101 &= 1 \cdot 6717425 + 1141676 && = 244526 \cdot 7859101 - 286085 \cdot 6717425 \\
6717425 &= 5 \cdot 1141676 + 1009045 && = 244526 \cdot 1141676 - 41559 \cdot 6717425 \\
1141676 &= 1 \cdot 1009045 + 132631 && = 36731 \cdot 1141676 - 41559 \cdot 1009045 \\
1009045 &= 7 \cdot 132631 + 80628 && = 36731 \cdot 132631 - 4828 \cdot 1009045 \\
132631 &= 1 \cdot 80628 + 52003 && = 2935 \cdot 132631 - 4828 \cdot 80628 \\
80628 &= 1 \cdot 52003 + 28625 && = 2935 \cdot 52003 - 1893 \cdot 80628 \\
52003 &= 1 \cdot 28625 + 23378 && = 1042 \cdot 52003 - 1893 \cdot 28625 \\
28625 &= 1 \cdot 23378 + 5247 && = 1042 \cdot 23378 - 851 \cdot 28625 \\
23378 &= 4 \cdot 5247 + 2390 && = 191 \cdot 23378 - 851 \cdot 5247 \\
5247 &= 2 \cdot 2390 + 467 && = 191 \cdot 2390 - 87 \cdot 5247 \\
2390 &= 5 \cdot 467 + 55 && = 17 \cdot 2390 - 87 \cdot 467 \\
467 &= 8 \cdot 55 + 27 && = 17 \cdot 55 - 2 \cdot 467 \\
55 &= 2 \cdot 27 + 1 && 1 = 55 - 2 \cdot 27
\end{aligned}$$

A signature is therefore 7573016.