Queen Mary
University of London

MTH6115 **Cryptography**
Exam Solutions **2012**

---

1. (a) A substitution cipher uses a permutation on the alphabet, while a transposition uses a permutation on the plaintext itself (i.e., rearranges the letters in the plaintext). To confuse digram frequency analysis one uses a transposition cipher.

   (b) One answer is $x \mapsto x+9$. Another answer is $x \mapsto 3x+7$.

   (c) The answer is: WMV RHY OKBXW RHYJ GTQW

   (d) They are the same. When we compose affine, substitution, and another affine, the outcome is simply a substitution cipher (for a certain permutation of the alphabet).

   (e) Such a ciphertext can be thought of as having been obtained by first subdividing the plaintext into m substring (where m is the length of the Vigenère key), then applying an affine substitution to each of these strings, and finally putting everything back together. So the Kasiski's method can be applied, keeping in mind that on each substring we have an affine substitution rather than a Caesar shift (but, frequency analysis still applies). One should also keep in mind that the affine ciphers differ by shifts.

2. (a) The answer is 'good luck with your final exams'. The ciphertext is obtained from this by applying a Caesar shift of size 6.

   (b) Suppose θ is given by $x \mapsto ax+b$ and θ' is given by $x \mapsto a'x+b'$. The letters c and f correspond to 2 and 5, respectively. So, by assumption, we have:

$$\begin{cases} 2a+b & \equiv & 2a'+b' \pmod{26} \\ 5a+b & \equiv & 5a'+b' \pmod{26} \end{cases}$$

   Subtracting, we find $3a \equiv 3a' \pmod{26}$. Since 3 is coprime to 26, we deduce that $a \equiv a' \pmod{26}$. Substituting this back in the first equation, we find that $b \equiv b' \pmod{26}$.

   (c) The encryption function for the Vigenère is not a one-way function. In other words, the decryption function is 'easy' to compute.

   (d) Alice decrypts the message using her own key, adds a preamble saying something like 'This is from Alice,' then encrypts the whole thing using Bob's key and sends it to Bob. Bob first decrypts the message using his secret key (at

this point he sees the message 'This is from Alice'), then he encrypts the message using Alice's key to get the actual message.

Since getting the actual message requires Bob to *encrypt* using Alice's key, it means at some point the message had been decrypted by Alice. (Here we use the assumption that $e \circ d$ is the identity operation.) Since this is a hard computation (unless one has access to the Alice's secret key), Bob can be fairly sure that it was Alice who did the computations.

(e) A function $f : A \to B$ is a 'one-way function' if it is 'easy' to compute f but 'hard' to compute the inverse of f. We say that f is a 'trapdoor one-way function' if there is an extra piece of information which makes it 'easy' to compute the inverse of f. In public-key cryptography, the encryption function $e : \mathcal{P} \times \mathcal{K} \to \mathcal{Z}$ is a trapdoor one-way function. The extra piece of information which makes the computation of the "inverse" for f 'easy' is the secret key.

3. (a) An n-bit shift register is a device holding n bits of data, which change at each tick of a clock. If these n bits are $x_0, \ldots, x_{n-1}$ prior to the tick of the clock, then afterwards we output x_0, and the n bits are $x_1, \ldots, x_n$, where

$$x_n = \sum_{i=0}^{n-1} a_i x_i \pmod 2,$$

where the a_i's, which are either 0 or 1 are constants associated with the shift register. The associated $\mathbb{Z}_2$ polynomial is $x^n + \sum_{i=0}^{n-1} a_i x^i$ (strictly $x^n - \sum_{i=0}^{n-1} a_i x^i$).

(b) There are $\frac{1}{5}\phi(2^5 - 1) = 6$ primitive and $\frac{1}{5}(-2 + 2^5) = 6$ irreducible polynomials. Since every primitive polynomial is irreducible, our counting shows that the set of primitive polynomials coincides with the set of irreducible polynomials.

For degree 4 polynomials, we have seen in class that $x^4 + x^3 + x^2 + x + 1$ is irreducible but not primitive.

(c) The output sequence is $000[001001000][...][...]$, where the part in bracket repeats. Since the period is $9 < 2^6 - 1$, the shift register is not primitive.

(d) First we determine the shift register. Let a_0, a_1 and a_2 be the coefficients of the shift register. We have the following system of equations:

$$\begin{cases} a_1 + a_2 &= 1 \\ a_0 + a_1 + a_2 &= 0 \\ a_0 + a_1 &= 0 \end{cases}$$

whose solution is $a_0 = 1$, $a_1 = 1$ and $a_2 = 0$. The output is $011100\underline{101}$.

4. (a) A $q \times q$ Latin square is a $q \times q$ array whose entries are taken from an alphabet of q symbols such that each symbol occurs precisely once in each row, and once in each column.

   (b)

a	b	c	d
b	c	d	a
c	d	a	b
d	a	b	c

   (c) $a \oplus b = c$, $(a \oplus d) \oplus c = d$, $a \ominus c = a$.

   (d) The adjugate is

d	c	a	b
a	d	b	c
b	a	c	d
c	b	d	a

   (e) **Shannon's Theorem** Suppose that Alice uses a one-time pad. Then, Eve's probabilities satisfy

$$P(p = P_0 \mid z = Z_0) \;=\; P(p = P_0);$$

   in other words, knowledge of the ciphertext gives no information about the plaintext.

   Proof Suppose Alice uses a one-time-pad. Then Eve's probabilities satisfy $\mathrm{P}(p = P_0 \mid z = Z_0) = \mathrm{P}(p = P_0)$, where Eve reckons the plaintext is P_0 with probability $\mathrm{P}(p = P_0)$ before intercepting the ciphertext $z = Z_0$, and that the plaintext is P_0 with probability $\mathrm{P}(p = P_0 \mid z = Z_0)$ after the interception. In what follows $\mathscr{P}$ is the set of all possible plaintexts, $\mathscr{K}$ is the set of keys, and $\mathscr{Z}$ is the set of all possible ciphertexts; these all have size q^m for a length m text. We have (using twice the fact that the substitution table is a Latin square):

$$\begin{aligned}
\mathrm{P}(z = Z_0) &= \textstyle\sum_{P_0 \in \mathscr{P}} \mathrm{P}(z = Z_0 | p = P_0).\mathrm{P}(p = P_0) \qquad \text{(Thm of Tot Prob)} \\
&= \textstyle\sum_{P_0 \in \mathscr{P}} \frac{1}{q^m}.\mathrm{P}(p = p_0) \qquad \text{(There is only one key } K_0 \text{ with } P_0 \oplus K_0 = Z_0) \\
&= \tfrac{1}{q^m} \textstyle\sum_{P_0 \in \mathscr{P}} \mathrm{P}(p = p_0) = \tfrac{1}{q^m},
\end{aligned}$$

   and

$$\begin{aligned}
\mathrm{P}(p = P_0 \mid z = Z_0) &= \tfrac{\mathrm{P}(p=P_0 \,\&\, z=Z_0)}{\mathrm{P}(z=Z_0)} = \tfrac{(1/q^m)\mathrm{P}(p=P_0)}{\mathrm{P}(z=Z_0)} \qquad \text{(since subst table Latin sq)} \\
&= \tfrac{(1/q^m)\mathrm{P}(p=P_0)}{1/q^m} = \mathrm{P}(p = P_0).
\end{aligned}$$

5. (a) Assume that Alice wants to send a secret message to Bob. Alice and Bob agree on a modulus p, a prime number. They must share the prime p, so they must assume that Eve know it. Each of them chooses a number coprime to $\lambda(p) = p-1$, and computes its inverse. These numbers are not revealed. Alice chooses d_A and e_A, Bob chooses d_B and e_B. Note that the commutation condition is satisfied:

$$T_{d_A}T_{d_B}(x) = x^{d_A d_B} \pmod{p} = T_{d_B}T_{d_A}(x).$$

Now Alice takes the message x and applies T_{e_A}; she sends $T_{e_A}(x)$ to Bob. Bob applies T_{e_B} and returns $T_{e_B}T_{e_A}(x)$ to Alice. Alice applies T_{d_A} and returns

$$T_{d_A}T_{e_B}T_{e_A}(x) = T_{d_A}T_{e_A}T_{e_B}(x) = T_{e_B}(x)$$

to Bob, who then applies T_{d_B} and recovers $T_{d_B}T_{e_B}(x) = x$, the original message.

(b) Suppose instead of the encryption and decryption functions $T_{e_A}(x) = x^{e_A}$ and $T_{d_A}(x) = x^{d_A}$, Alice used a one-time pad, i.e., $D_A(x) = x \oplus_A k_A$ and $E_A(x) = x \ominus_A k_A$, where Alice has chosen a Latin square $\oplus_A$ and a random key k_A. (Similarly for Bob. We must assume that $\oplus_A$ and $\oplus_B$ commute, in the sense that $x \oplus_A y \oplus_B z = x \oplus_B z \oplus_A y$. This is the case with binary addition. We also assume that Eve knows $\oplus_A$ and $\oplus_B$.) Then, during the key-exchange process, Eve would get hold of the following:

$$D_A(x) = x \oplus k_A,\ D_B D_A(x) = x \oplus_A k_A \oplus_B k_B,\ D_B(x) = x \oplus_B k_B.$$

From the first two, Eve can recover k_B. Then, she can use k_B with the thrid one to recover x.

[Students have seen this in the case where $\oplus_A$ and $\oplus_B$ are both binary addition. It is OK if they only explain this case.]

(c) The residue of division of 2829 by $2 \cdot 680 = 1360$ is $r = 109$. Therefore, the prime factors of 2829 are the roots of the polynomial

$$x^2 - (r+1)x + n = x^2 - 110x + 2829.$$

This is an easy equation to solve (even without a calculator). The answer is $2829 = 41 \cdot 69$.

(d) We have $de - 1 = 132 = 4 \cdot 33$. Apply the algorithm with $x = 2$. We have $\gcd(2, 299) = 1$. Let $y = 70 \equiv 2^{33} \pmod{299}$. (Note that $2^{33} \pmod{299}$ is easy to calculate because $33 = 2^5 + 1$.) Then $z = 70^2 \equiv 116 \pmod{229}$ has the property that $z^2 \equiv 1 \pmod{299}$. So 299 divides $116^2 - 1 = 115 \cdot 117$. From this we find the factors of 299 to be $\gcd(115, 299) = 23$ and $\gcd(117, 299) = 13$. So, $299 = 13 \cdot 23$.

6. (a) The discrete logarithm problem is the following

   Given x, y, and a prime p such that $y \equiv x^e \pmod{p}$, find e.

   It is not known to be NP-complete. El-Gamal crypto-system is based on this problem.

   (b) Since 43 is prime, the order k of 2 modulo 43 should divide $43-1 = 42 = 2 \cdot 3 \cdot 7$. It is easy to see that k can not be any of 2, 3, 6, and 7. In fact $2^7 \equiv -1 \pmod{43}$. So the order of 2 is $k = 14$.

   (c) This is an element $g \in \mathbb{Z}_p$ whose order is precisely $p-1$.

   (d) First we show that if g is a primitive root modulo p then g^k is a primitive root if and only if $\gcd(k, p-1) = 1$. First suppose that $\gcd(k, p-1) = 1$. We want to show that $h := g^k$ is a primitive root. There exists l such that $lk \equiv 1 \pmod{p-1}$. So, by Fermat, $h^l = g^{kl} \cong g \pmod{p}$. Since g is a power of h, and every $x \in \mathbb{Z}_p$ is a power of g, every such x is a power of h as well. To prove the converse, suppose that $h = g^k$ is a primitive root. Let $d = \gcd(k, p-1)$. Then, $h^{\frac{p-1}{d}} = g^{k\frac{p-1}{d}} \equiv 1 \pmod{p-1}$. Since h is a primitive root, this implies that $\frac{p-1}{d} \geq p-1$. Therefore, $d = 1$.

   (e) First we need to find one primitive root. The first guess is $g = 2$. The order k of 2 divides 10. It is easy to see that k is not any of 1, 2, or 5, so $k = 10$. This shows that $k = 10$, that is, 2 is a primitive root. Now, by the previous part, the primitive roots modulo 11 are

$$\{2^1, 2^3, 2^7, 2^9\} = \{2, 8, 7, 6\}.$$