CS555: Cryptography **Spring 2012**

Homework #1

Due date & time: 10:30am on January 26, 2012. Hand in at the beginning of class (preferred), or email to the TA (jiang97@purdue.edu) by the due time.

Late Policy: You have three extra days in total for all your homeworks. Any portion of a day used counts as one day; that is, you have to use integer number of late days each time. If you emailed your homework to the TA by 10:30am the day after it was due, then you have used one extra day. If you exhaust your three late days, any late homework won't be graded.

Additional Instructions: The submitted homework must be typed. Using Latex is recommended, but not required.

Problem 1 (25 pts) Write a program that breaks the Vigenère cipher automatically. That is, assuming that the plaintext is a case-insensitive English text using only the 26 letters (without space or any other symbol), your algorithm should take in a ciphertext encrypted under the Vigenère cipher, and automatically output the plaintext.

Hint. For telling whether a shift value is correct, you can consult the paragraph titled "An improved attack on the shift cipher" in the textbook on Pages 13–14. You are encouraged to come up with a different way for doing this as well.

- Include the core part of the source code of your implementation (leave out input processing), and state the language you use. Also email a zip file of your source code to the TA.
- Present the plaintext for the attached ciphertext file, computed using your program.
  Ciphertext: (Use the latex source file for the ciphertext.)

```
rimqessfntwpwtelqdeerkwdpezrfxjumpqxqqurxhifdjaffirlffnsyahrxtou
tszwaxwvdspwqbpidwhitvpdnvizstnexzrhpujfcwmfvihdcspkqbrvpczztxug
nfdlhdzreheyrkworezrnrpcmatrsdesifqpwwfvnxdmssnsysgltzbgwyqbpidw
oegidgnvxvgbyhivvgwrffcixogiskcwlvuchwpjdfnxewamcwcsxefwbrhvqvcm
fmfyryotoefopscwweprfwnpxkmelxmwaxtxfjecmbqejkvfyxuqnxxfbnzhqfag
gpduzkdoclnzbupvespxhkvfomeqvtazbfdsranxwvabemogpsbgiupveqvictsb
yhqzrgiiwdlpqbtmcvsstrsoctazqbemabfsutfzaxaueeeymjygxiqipkadlvpg
psbgiupvbofwlffedezrrptthszruqpsbdssniofltifzprcbfvsgkcusiycqige
ohpamgnpbfgudczcacbfithmfvrrrimqemabglttcogidgvscftjyjafzeizcoqv
aanvtrrbmpqggeivhpltboeickbpywqbfiiystprpsevtkojyiphuipswmtxkhbh
ttfzaxfvrmcwcsxefwbrperusidsssgvowzmpiaapehfotqffscjpftrsooptkcs
pepwgwxeqfhsdzqapiwbyhfvresmsoesrhuirfaqfxqfgltdsusspghwtuhpnedf
lsjkqsjtfcysvpvbginspsbvwonvqofmcxzznsydyimrbetxeoctazqbemabzsgv
kjoiedeipuapoidbpvnghprvmducufzmzaeofxgfbhwceqvickwgtgmdcvdrqilr
prrwxxbtnvkdgsvioqsmooykdiwusqeoesjerdzqbigeizcolptoehcvgtlweizt
izcodqmyvrvjidsexubvxkvndlmfqxdsfflonmnrpujfcwmflmizgusiafrxxtom
wcbcfwxszfesnfrezjidseemfxtdpvemfwfmcwsbdmnzrxductzfkoaceiodemoo
yqtrbtelqgrwrysnpwmfrxwvffqsdspsbgiulxucaeacmtpggfrxwvffpbuggmcw
```

```
csxefwbriyspcifwpeacmtpggfrwrysnpwfvnxeicwlfxmpececuminfboteoopb
macptzgusiabrxxdsqlhnigxwvgfdgtszihrffxsdsqmuwwdfpfhbmbgzfxizhgl
pehipxtsbvtkwdlpxmovtrybmpqphxrfaqfxmhvscrzmjwqqhvtdsdsezwfqhtfz
axazbknismlxqrgirybpwssmuehiojdipoaybssszjxsteazgtfiewaxwviotxqr
xmcxrpxeprvxxfbtesfvrvtximlxucasuzbwpwfwteiffzasisewpthspugweihr
gvdtqqgistfjxmzoyxdyoooshsexwvwsprofltizcovikwsehbsemcxojicwcsni
ysaxdkvfcaugrxwvitpviwypurqflgdwzmcrzdsedurxwvsmpgffbrxttszrfwrv
ufiooefwbrxjwogsxjrhxeodlwqwaxwvgvavqargdlfuzjfvryczhfowfogihnvj
nliwyppjqfcxmwamuisrfmdwakhlgqpgfsqggzajyexggseicwthqhuixisonvkd
gmdeyfjwfcyelvbgzvoszickwtfrocawizhvemabnpiysfqjugnvvlworxtogxwz
gjdehwbppkwpysrhuigzuiesrbbxqvworjafpiskcjygdwzmcrhfzrqgrpurghtz
qbvriysgtjfvnqternprf
```

Problem 2 (5 pts) Consider the following enhancement of the Vigenère cipher. We again assume that the plaintext is a case-insensitive English text using only the 26 letters (without space or any other symbol). To encrypt a plaintext m of length n, one first uniformly randomly generate a string over the alphabet $[A..Z]$ of length 13. Then insert this string into the beginning of the plaintext. That is, we construct a string $x = x_1x_2 \dots x_{n+13}$, such that $x_1 \cdots x_{13}$ is the string we have generated, and $x_{14} \cdots x_{n+13}$ is the plaintext string. We then construct a string y as follows: $y_i = x_i$ for $1 \le i \le 13$, and for $i \in [14, n+13]$, y_i is the result of using y_{i-13} to encrypt x_i; that is, when the x_i's and y_i's are treated as numbers in $[0..25]$, we have $y_i = ((x_i + y_{i-13}) \mod 26)$. We then apply the Vigenère cipher to the string y, making sure that the key length is not a multiple of 13.

- Write the Pseudo-code of the algorithms Enc,Dec for this cipher.

  Note that this cipher offers randomized encryption. The same plaintext encrypted twice result in different ciphertexts. Also note that the ciphertext of a plaintext is always 13 characters longer than the plaintext. This is necessary for randomized encryption.

- **Optional Question. No credit.**

  Describe how you would break the above encryption scheme.

  Do it only if you have the time and enjoy doing it. The instructor does not know the answer. If you are able to break the cipher, the solution will be presented in class. You get to present it if you choose to do so.

Problem 3 (10 pts) Consider an encryption scheme in which $\mathcal{M} = \{a, b, c\}$, $\mathcal{K} = \{K_1, K_2, K_3\}$ and $\mathcal{C} = \{1, 2, 3, 4\}$. The keys are chosen uniformly randomly; in other words, $\mathbf{Pr}[\mathsf{Key} = K_1] = \mathbf{Pr}[\mathsf{Key} = K_2] = \mathbf{Pr}[\mathsf{Key} = K_3] = 1/3$, and the encryption matrix is as follows:

	a	b	c
K_1	1	2	3
K_2	2	3	4
K_3	3	4	1

- Assuming the plaintext distribution in which each plaintxt is chosen with the same probability, i.e., $\mathbf{Pr}[\mathsf{PT} = a] = \mathbf{Pr}[\mathsf{PT} = b] = \mathbf{Pr}[\mathsf{PT} = c] = \frac{1}{3}$.

- **(2 pts)** Compute the probability distribution of the ciphertext CT, that is, give the probabilities for $\mathbf{Pr}[\mathsf{CT} = 1]$, $\mathbf{Pr}[\mathsf{CT} = 2]$, $\mathbf{Pr}[\mathsf{CT} = 3]$, $\mathbf{Pr}[\mathsf{CT} = 4]$.
- **(2 pts)** Compute the joint distribution of PT and CT, by filling out a table like the one below.

	$\mathsf{PT} = a$	$\mathsf{PT} = b$	$\mathsf{PT} = c$
$\mathsf{CT} = 1$	$\frac{1}{9}$		
$\mathsf{CT} = 2$			
$\mathsf{CT} = 3$			
$\mathsf{CT} = 4$			

- **(1 pt)** Are PT and CT independent?

- **(5 pt)** Repeat the questions above, assuming the following plaintext distribution, $\mathbf{Pr}[\mathsf{PT} = a] = \frac{1}{2}$, $\mathbf{Pr}[\mathsf{PT} = b] = \frac{1}{3}$, $\mathbf{Pr}[\mathsf{PT} = c] = \frac{1}{6}$.

Problem 4 (16 pts) Read Chapter 1 of the PDF file "Mathematics for Computer Science" by Lehman and Leighton. (Available from http://www.cs.princeton.edu/courses/archive/spr10/cos433/mathcs.pdf)

- **(2 pts)** Check whether the following statements are propositions.
  - (a) 1,2 and 3 are prime numbers.
  - (b) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x^2 - x + 1 > y$.
  - (c) Let's try to prove the existence of pseudorandom generators!
  - (d) Let $a, b > 1$ with $b \nmid a$, then $gcd(a, b) = gcd(b, a \bmod b)$.
- **(4 pts)** Check whether the following propositions are tautology.
  (P, Q, R are boolean variables)
  - (a) $P \wedge \neg P \Rightarrow Q$
  - (b) $(P \Rightarrow Q) \Leftrightarrow \neg P \vee Q$
  - (c) $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$
  - (d) $(P \Rightarrow Q) \wedge (R \Rightarrow \neg Q) \wedge R \Rightarrow \neg P$
- **(8 pts)** Prove the following propositions.
  - (a) (2 pts) A complete number is not a prime number.(Note: complete number refers to a number which is equal to the sum of its proper divisors. For example, 6 and 28 are complete numbers since $6 = 2 \times 3 = 1 + 2 + 3, 28 = 2 \times 2 \times 7 = 1 + 2 + 4 + 7 + 14$.)
  - (b) (3 pts) For all $n \geq 4$, $2^n < n! < n^n$
  - (c) (3 pts) There is no rational number x for which $x^3 + x + 1 = 0$.
    Hint: a rational number can be written as a/b such that a and b are not both even numbers.
- **(2 pts)** Order the following functions in terms of their growth: $\log n$, $n^{\log n}$, n^{100}, 1.1^n, e^n, $n!$.
  This is not related to the reading here, but serves as a review for concepts used in later topics. Consult, for example, wikipedia page on big-o notation if you are unfamiliar with this.

Problem 5 (9 pts) This question asks you to consider the relationship between keyspace size $|\mathcal{K}|$, plaintext space size $|\mathcal{M}|$, ciphertext space size $|\mathcal{C}|$, for symmetric ciphers, which we require that

$$\forall m \forall k \mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m.$$

- For the pair $(|\mathcal{M}|, |\mathcal{C}|)$, identify which of the following choice is true, and show that your answer is correct.
  - (a) It must be that $|\mathcal{M}| = |\mathcal{C}|$.
  - (b) It must be that $|\mathcal{M}| \geq |\mathcal{C}|$, and it is possible that $|\mathcal{M}| > |\mathcal{C}|$.
  - (c) It must be that $|\mathcal{M}| \leq |\mathcal{C}|$, and it is possible that $|\mathcal{M}| < |\mathcal{C}|$.
  - (d) Each of the following is possible: $|\mathcal{M}| > |\mathcal{C}|$, $|\mathcal{M}| = |\mathcal{C}|$, and $|\mathcal{M}| < |\mathcal{C}|$.
  - (e) None of the above is true.
- Choose among (a)-(e) for the pair $(|\mathcal{M}|, |\mathcal{K}|)$, and justify your answer.
- Choose among (a) -(e) above for the pair $(|\mathcal{C}|, |\mathcal{K}|)$, and justify your answer.

Problem 6 (9 pts) Repeat the previous problem for a symmetric-key cipher that satisfies perfect secrecy.

Problem 7 (6 pts) (Katz and Lindell. Page 41. Problem 2.5.)
Prove or refute: Every encryption scheme for which the size of the key space equals the size of the message space, and for which the key is chosen uniformly from the key space, is perfectly secret.

Problem 8 (10 pts) (Katz and Lindell. Page 42. Problem 2.7.)
Prove that Definition 2.1 implies Definition 2.4.

Def. 2.1: An encryption scheme (Gen,Enc,Dec) over a message space $\mathcal{M}$ is perfectly secret if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\mathbf{Pr}[C = c] > 0$: $\mathbf{Pr}[M = m | C = c] = \mathbf{Pr}[M = m]$.
Def. 2.4: An encryption scheme (Gen,Enc,Dec) over a message space $\mathcal{M}$ is perfectly secret if for every adversary $\mathcal{A}$ it holds that $\mathbf{Pr}[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}$.

Hint from textbook. Use Exercise 2.6 to argue that perfect secrecy holds for the uniform distribution over any two plaintexts(and in particular, the two messages output by $\mathcal{A}$ in the experiment). Then apply Lemma 2.3.

Exercise 2.6: Say encryption scheme (Gen,Enc,Dec) satisfies Definition 2.1 for all distributions over $\mathcal{M}$ that assign non-zero probability to each $m \in \mathcal{M}$ (as per the simplifying convention used in this chapter). Show that the scheme satisfies the definition for all distributions over $\mathcal{M}$ (i.e. including thoes that assign zero probability to some messages in $\mathcal{M}$). Conclude that the scheme is also perfectly secret for any message space $\mathcal{M}' \subset \mathcal{M}$.

Lemma 2.3: An encryption scheme (Gen,Enc,Dec) over a message space $\mathcal{M}$ is perfectly secret if and only if for every probability distribution over $\mathcal{M}$, every $m_0, m_1 \in \mathcal{M}$, and every $c \in \mathcal{C}$: $\mathbf{Pr}[C = c | M = m_0] = \mathbf{Pr}[C = c | M = m_1]$.

Problem 9 (10 pts) (Katz and Lindell. Page 42. Problem 2.8.)

Prove the second direction of Proposition 2.5. That is, prove that Definition 2.4 implies Definition 2.1.

Hint. If a scheme Π is not perfectly secret with respect to Definition 2.1, then Lemma 2.3 shows that there exist messages $m_0, m_1 \in \mathcal{M}$ and $c \in \mathcal{C}$ for which $\mathbf{Pr}[C = c|M = m_0] \neq \mathbf{Pr}[C = c|M = m_1]$. Use these m_0 and m_1 to construct an $\mathcal{A}$ for which $\mathbf{Pr}[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] > \frac{1}{2}$.