

Assignment 2
Computer Science 349
Spring 2004

Due: Start of class on Thursday February 12

Reading: Singh, Chapters 2, 3; Stinson, Sections 1.1.3 -- 1.1.7, 1.2.1 – 1.2.2.

Exercise 2.0. Read the article by Robert Lemos, “Psst ... I know your password”, ZDNet News, May 22, 2002. URL: <http://zdnet.com.com/2100-1105-920092.html> and the article by Rob Shimonski, “Introduction to Password Cracking”, IBM developerWorks Hacking Techniques, July 2002. URL: <http://www-106.ibm.com/developerworks/security/library/s-crack> .



Experiment with John the Ripper (a.k.a. John) in an attempt to crack (some) passwords contained in a mock `/etc/passwd` file which may be downloaded from the course web page. Source code John may be found from <http://www.openwall.com/john/>. Program documentation is located at the same site as the program. Warning: Under no circumstances should you attempt to run John on password files other than those given in this assignment.

By default, John uses the word list in `password.lst` in the same directory as the binary file. This is not a very extensive word list. You may want to combine it with a larger word list, such as the one in `/usr/share/dict/linux.words`. You might also want to include Wellesley-specific words, which you could potentially automatically generate from some documents about the campus. Note that John takes a long time to run (we’re talking days) – indeed, it may never terminate on its own and you may have to manually terminate it.

A gold star goes to the student who cracks the most passwords. As a baseline, you will have to beat 15, which is how many I cracked after running the program for 10 minutes. Submit your list of cracked passwords and associated users accounts as the solution to this exercise. Did you recognize any of your own passwords?¹

Exercise 2.1. (Stinson 1.6) If an encryption function e_K is identical to the decryption function d_K , then the key K is said to be an involutory key. Find all involutory keys in the *Shift Cipher* over Z_{26} .

¹ The hash function used to create these accounts used only the first eight characters of your password. It was very bad of me not to tell you this in advance.

Exercise 2.2. (Stinson 1.10) Suppose that $K = (5, 21)$ is a key in an *Affine Cipher* over \mathbb{Z}_{29} .

- Express the decryption function $d_K(y)$ in the form $d_K(y) = a'y + b'$, where $a', b' \in \mathbb{Z}_{29}$.
- Prove that $d_K(e_K(x)) = x$ for all $x \in \mathbb{Z}_{29}$.

Exercise 2.3. In one of his cases, Sherlock Holmes was confronted with the following message:

534 C2 13 127 36 31 4 7 21 41
DOUGLAS 109 293 5 37BIRLSTONE
26 BIRLSTONE 9 127 171

Watson, still working his way through Holmes's little monograph on codes and ciphers. was stumped. Fortunately, Holmes immediately deduced the type of cipher. Having read Chapter 2 of Singh, so can you. What is it?

Exercise 2.4. Sherlock Holmes was not the first investigator to benefit from cryptanalysis. Some years before *The Adventure of the Dancing Men* was published, Mr. William Legrand, stumbled upon Captain Kidd's treasure map complete with skull and goat's head. The fact that the map was written in invisible ink presented some small problem:

"I held the vellum again to the fire, after increasing the heat, but nothing appeared. I now thought it possible that the coating of dirt might have something to do with the failure: so I carefully rinsed the parchment by pouring warm water over it, and, having done this, I placed it in a tin pan, with the skull downward, and put the pan upon a furnace of lighted charcoal. In a few minutes, the pan having become thoroughly heated, I removed the slip, and, to my inexpressible joy, found it spotted, in several places, with what appeared to be figures arranged in lines. Again I placed it in the pan, and suffered it to remain another minute. Upon taking it off, the whole was just as you see it now."

The figures, transcribed from the rudely drawn originals, appear below:

5 3 † † † 3 0 5)) 6 * ; 4 8 2 6) 4 † .) 4 †) ; 8 0 6 * ; 4 8 † 8 † 6 0))
8 5 ; 1 † (; : † * 8 † 8 3 (8 8) 5 * † ; 4 6 (; 8 8 * 9 6 * ? ; 8) * † (; 4 8
5) ; 5 * † 2 : * † (; 4 9 5 6 * 2 (5 * - 4) 8 † 8 * ; 4 0 6 9 2 8 5) ;) 6 †
8) 4 † † ; 1 († 9 ; 4 8 0 8 1 ; 8 : 8 † 1 ; 4 8 † 8 5 ; 4) 4 8 5 † 5 2 8 8 0 6 *
8 1 († 9 ; 4 8 ; (8 8 ; 4 († ? 3 4 ; 4 8) 4 † ; 1 6 1 ; : 1 8 8 ; † ? ;

The code is a simple substitution; apparently Captain Kidd didn't have a high opinion of his crew's cryptographic skills. Using the frequency table given in the text, can you figure out what it says? *Warning:* The resulting message is in English but may not make much sense on a first reading. It has a history.

Exercise 2.5. The following mystery story is from Games magazine.² The idea is not to guess "who did it," because it is the author "who's done it." The problem is to figure out exactly what he has done.

A SIN OF OMISSION

Around midnight, a sly-looking man slips into a luxury city building. A woman occupant, watching his actions from a fourth-floor window, grows suspicious and dials 911 for a patrol car. This lady complains, "A man in a brown suit, with shaggy hair, a slight build, and a criminal air is prowling through my lobby."

Fairly soon two young cops, Smith and Jarvis, pull up. Looking for an unknown vagrant, Smith spots Jim Oats walking out a front door. Oats, a minor burglar, is bold as brass, arrogant, and calm. Smith grabs him by his collar.

"O.K, Oats," snarls Smith, "What brings you to this location?"

"Fixing his captor with a chilly look and frosty indignation, Oats quips, "I can go on a short stroll. Lift your filthy hands off my shirt. I'm not guilty of anything."

Smith drops his hands limply. This haughty air is too much for him to swallow. Angrily Smith says, "What a story. I'm nobody's fool, you punk. I just wish I could put you back in jail, but I can't obtain any proof against you. You know all about why I'm in this building -- a station log full of burglary, arson, and muggings."

"Now, now," Oats laughs, "think of my rights. How can you talk this way?" Smith's probing hands start to frisk Oats for guns, narcotics, anything unlawful or contraband. Nothing shows up -- only a small bound book. "That's this?" Smith asks.

Oats, tidying up his clothing, pluckishly says, "That's my political study of about habits in this district. Why don't you look at my lists? I work for important politicians now -- guys with lots of clout." An ominous implication lurks in this last thrust.

"Don't talk down to us," Smith snaps. But studying Oat's book, Jarvis finds nothing unusual. Smith finally hands him back his lists. Our cops can't hold him. Jarvis admits Oats can go. Just as a formality, Jarvis asks him, "Did you commit any criminal act in this building? Anything at all of which a courtroom jury could find you guilty?"

"No," Oats says flatly. "No way," and jauntily skips off. Halting six blocks away, Oats digs a tiny picklock from his sock and a diamond ring from his shaggy hair.

Exercise 2.7. One way to solve the key distribution problem is to use a line from a book that both the sender and the receiver possess. Typically, at least in spy novels, the first sentence of a book serves as the key. The particular scheme discussed in this problem is from the suspense novel, *Talking to Strange Men*, by Ruth Rendell. Work this problem without consulting that book! Consider the following message:

SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA

This ciphertext was produced using the first sentence of the *The Other Side of Silence* (a book about the spy Kim Philby);
The snow lay thick on the steps and the snowflakes driven by the wind looked black in the headlights of the cars.

² Games magazine, November/December 1977.

A simple substitution cipher was used. What is the encryption algorithm? How secure is it? To make the key distribution problem simple, both parties can agree to use the first or last sentence of a book as the key. To change the key, they simply need to agree on a new book. The use of the first sentence would be preferable to the use of the last. Why?