DEPARTMENT OF EECS

Indian Institute of Technology Bhilai

CS553 – CRYPTOGRAPHY

Semester: 2022-M

Scope: Classical Ciphers, Attack Models, Perfect Secrecy, SageMath

Assignment 2

August 13, 2022

- Instructions
  - LaTeX based answers are preferred
  - "Readme" file for your code (if applicable)
  - Submissions in a zip file named as `<group-name>_<assignment_no>`
  - This is a running assignment. More problems will be added and you will be notified

1 Classical Ciphers

1. A *homophonic cipher* is a substitution cipher in which there may be more than one ciphertext symbol for each plaintext letter. Here is an example of a homophonic cipher, where the more common letters have several possible replacements.

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
!	4	#	$	1	%	&	*	(	)	3	2	=	+	[	9	]	{	}	:	;	7	<	>	5	?
♡	○	⋆	ℵ	6	↗	▷	◇	∧			↘	Δ	∇	8	♣		Ω	∨	⊗	♠				♭	
Θ				∞		⇑		♮					●	⊙				◁	⊕	⇐					
↙				⇓														⇒	↖						

   Decrypt the following message.

   (% Δ ♠ ⇒ ♮ # 4 ∞ : ◇ 6 ↗ ⊙ [ℵ 8 % 2 [7 ⇓ ♣ ↘ ♡ 5 ⊙ ∇

2. Decrypt each of the following Caesar encryptions by trying the various possible shifts until you obtain readable text.

   (a) LWKLQNWKDWLVKDOOQHYHUVHHDELOOERDUGORYHOBDVDWUHH

   (b) UXENRBWXCUXENFQRLQJUCNABFQNWRCJUCNAJCRXWORWMB

   (c) BGUTBMBGZTFHNLXMKTIPBMAVAXXLXTEPTRLEXTOXKHHFYHKMAXFHNLX

   Write a program to automate the above process. Can you find if you got a readable text without manually reading it?

3. An affine cryptosystem is given by the following encryption function, where a, b are chosen from $\mathbb{Z}_{26}$.

$$enc_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$x \to ax + b \in \mathbb{Z}_{26}$$

- Encrypt the plaintext `cryptography` using the affine code $enc_{3,5}$. What is the decryption function corresponding to $enc_{3,5}$? Decrypt the ciphertext `XRHLAFUUK`.
- A central requirement of cryptography is that the plaintext must be computable from the key and the ciphertext. Explain why $enc_{2,3}$ violates this rule. Show that the function $enc_{a,b}$ satisfies the rule if and only if $gcd(a, 26) = 1$.
- In the following we consider only functions $enc_{a,b}$ with $gcd(a, 26) = 1$. Show that all affine codes with $b = 0$ map the letter a to a and the letter n to n.

4. A key is called involutory when $e_K = d_K$. Let an Affine Cipher be defined over $\mathbb{Z}_m$ with key $K = (a, b)$.

   - Prove that K is an involutory key if and only if

   $$a^{-1} \bmod m = a \text{ and } b(a+1) \equiv 0 \bmod m$$

   - Now find all involutory keys in $\mathbb{Z}_{15}$ for the Affine Cipher
   - Determine the number of keys in an Affine Cipher over $\mathbb{Z}_m$ for $m = 30, 100$ and 1225.

5. Consider the following variable of Hill cipher defined by

   $$e_k(m) \equiv k_1 \cdot m + k_2 (\text{mod} p) \qquad \text{and} \qquad d_k(c) \equiv k_1^{-1} \cdot (c - k_2)(\text{mod} p)$$

   where m, c, and k_2 are column vectors of dimension n, and k_1 is an $n-$by$-n$ matrix.

   (a) We use the vector Hill cipher with $p = 7$ and the key $k_1 = \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}$ and $k_2 = \begin{pmatrix} 5 \\ 4 \end{pmatrix}$

   - Encrypt the message $m = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$
   - What is the matrix k_1^{-1} used for decryption?
   - Decrypt the message$c = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$.

   (b) Explain why the Hill cipher is vulnerable to a known plaintext attack.

   (c) The following plaintext/ciphertext pairs were generated using a Hill cipher with the prime $p = 11$. Find the keys k_1 and k_2.

   $m_1 = \begin{pmatrix} 5 \\ 4 \end{pmatrix}$ $c_1 = \begin{pmatrix} 1 \\ 8 \end{pmatrix}$ $m_2 = \begin{pmatrix} 8 \\ 10 \end{pmatrix}$ $c_2 = \begin{pmatrix} 8 \\ 5 \end{pmatrix}$ $m_3 = \begin{pmatrix} 7 \\ 1 \end{pmatrix}$ $c_3 = \begin{pmatrix} 8 \\ 7 \end{pmatrix}$

   (d) Explain how any simple substitution cipher that involves a permutation of the alphabet can be thought of as a special case of a Hill cipher.

2 Introducing SageMath (https://www.sagemath.org/)

SageMath is a free open-source mathematics software system licensed under the GPL.

6. Encrypt the names of all members of your group with any three classical ciphers using Sage. Also write a case-study in cryptanalyzing any one of them. Do some research on this. Can you implement the cryptanalysis strategy you have chosen using Sage. The difficulty of the strategy you choose will decide the marks you score in this problem.

   Hint: `https://doc.sagemath.org/html/en/reference/cryptography/sage/crypto/classical.html`

3 Number Theory with SageMath

7. Implement the Euclidean GCD and Extended Euclidean GCD functions in Sage. Use them to write two wrapper functions to find number of invertible elements in $\mathbb{Z}_m$, given m and the inverse of any element in $\mathbb{Z}_m$ (Throw an error message if not invertible).

   - Sage also has in-built functions for solving the above problem. Redo it using inbuilt functions.

   Hint: Is there an alternative way to find number of invertible elements in $\mathbb{Z}_m$?

4 Perfect Secrecy

8. Suppose $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is a cryptosystem where $|\mathcal{K}| = |\mathcal{P}| = |\mathcal{C}|$, then the cryptosystem provides perfect secrecy if and only if every key is used with equal probability $1/|\mathcal{K}|$, and for every $x \in \mathcal{P}$ and $y \in \mathcal{C}$ there is a unique K such that $e_K(x) = y$.

   - Prove it. You are allowed to refer Stinson.