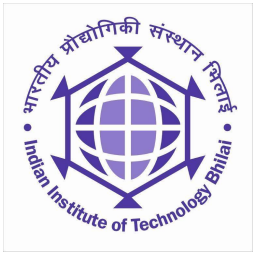

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
Indian Institute of Technology Bhilai
CS553/CSL505 – CRYPTOGRAPHY
Semester: 2024-M
Scope: Classical Ciphers, Sage Math, Perfect Secrecy

Assignment 2
August 22, 2024

- Instructions
  - LaTeX based answers are preferred
  - "Readme" file for your code (if applicable)
  - Submissions in a zip file named as `<group-name>_<assignment_no>`
  - Some problems are to be submitted in the notebook.

1 Capture The Flag

1. Demonstrate how you solved the CTF that lead you to this Assignment? If your group is among the first three teams then, you will receive bonus points. However, every group must justify how they got hold of this `pdf` file.

   ***Note**: If you are unable to justify this then the rest of the solutions will not be accepted.*

2 Classical Ciphers

2. 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 ⊙ ∇

3. 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?

4. 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.

5. 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.

6. The **Atbash** Cipher consists of replacing plaintext letters A, B, C to Z by the ciphertext letters Z, Y, X to A, respectively.

   - Decrypt 'XZKVIXZROORV.'
   - How would you describe the relationship between the Atbash Cipher and the Simple Substitution Cipher?

7. Recall the Vigenre Cipher discussed in class.

   - Encrypt MY HOME IS INDIA using a Vigenre Cipher with keyword KEA.
   - The ciphertext JNHYSMCDJOP was obtained by encrypting an English word using a Vigenre Cipher:
     - The first and ninth letters of the plaintext are identical. What does this tell you about the key?

  - Given the keyword length is less than 7, the third and fourth letters of the plaintext are F and O, respectively, and A is a letter in the keyword, find the keyword and the plaintext.
- If the keyword of a Vigenre Cipher has repeated letters, does this make it any easier to break?

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

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

8. 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`

4 Number Theory with SageMath

9. 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 $\mathbb{Z}_m$?

5 Perfect Secrecy [Notebook]

10. Find the flaw in the following argument:

    Consider the following attack against one-time pad: upon seeing a ciphertext c, the eavesdropper tries every candidate key $k \in \{0,1\}^n$ until she has found the one that was used, at which point she outputs the plaintext m. This contradicts the argument that the eavesdropper can obtain no information about m by seeing the ciphertext.

11. Solve and submit the two problems given in the Lecture Note on Perfect Secrecy.

6 TLS 1.3

12. As shown in CIA-1, using the `openssl` dumps with a local client-server compare and contrast TLS 1.2 and TLS 1.3. Submit all necessary files and a script to verify your approach.

    Now write a note in your **notebook** highlighting how TLS 1.3 improves upon TLS 1.2.
