



Brute Force Attacks

- 1- Let us assume there is a password-based authentication system. The password has 8 characters. In a brute force attack, the attacker tries all possible passwords to find the right one. Assume that an authentication takes $1 \mu s$.
 - a. All users only use small English letters and they use them in a uniform and random way. How much time does the attacker need on average?
 - b. Now assume that also capital letters, numbers and 31 ASCII special characters are used, so-called strong passwords. What is now the average time the attacker needs?
- 2- Consider the following algorithm that generates random passwords for new users on a system: It selects a character from the set of: English lowercase and uppercase characters, as well as the six punctuation characters $< > [] \{ \}$. How many passwords are possible if a 5 character long password is generated using this algorithm ?
- 3- The passwords a user can choose for a given system are:
 - At least 6 characters and at most 8 characters long
 - composed of characters from the following character set: lowercase letters a-z (size=26), uppercase letters A-Z (size=26), digits 0-9 (size=10), and special characters/symbols (size=32)Consider the following two password policies:
 - Policy 1: The user can freely choose his/her password
 - Policy 2: The password must at least have one digit or at least one special character
 - a) For each of the above two password policies, calculate the number of possible passwords
 - b) Based on the number of possible passwords and assuming an ideal user that randomly chooses passwords, which of these two policies seems more secure and why?
 - c) In fact, users rarely choose their passwords randomly, but stick to certain simple patterns that are easier to remember and to type. Let's assume the typical user, when he/she can freely choose her password (in Policy 1), will prefer passwords that consist only of lowercase and uppercase letters. What is the number of possible passwords for such a typical user?
 - d) Revisit the question 2 again.
- 4- Suppose that using commodity hardware it is possible to build a computer for about \$200 that can brute force about 10 billion AES keys per second. Suppose an organization wants to run an exhaustive search for a single 128-bit AES key and is willing to spend four trillion (4×10^{12}) dollars to buy these machines (this is about the annual US federal budget). How long would it take the organization to run an exhaustive search for this single 128-bit AES key with these machines, in the worst case? Ignore additional costs such as power and maintenance.

Random Substitution Cipher

- 5- Consider the message $m = HKPUFCMHY BHDDXZH$, and let (E, D) be a substitution cipher.

- a) Decrypt m using the following (secret) substitution key:

plaintext	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
ciphertext	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O

- b) Can this cipher be broken by someone who has access to m but not to the secret key? Why?



Affine Cipher

- 6- Consider the Affine Cipher with a plaintext space consisting of the English alphabet (small case letters), the space character and the ten digits (0-9). The characters values are assigned sequentially starting with the letter “a” (value 0) and ending with the digit “9”.
- What is the modulus to be used in the encryption process? Justify your answer
 - The key used in the affine cipher is $(a = 2, b = 3)$. Explain why this key is valid.
 - Encrypt the message “secu 301” using the above key $(3, 2)$
 - Write the decryption equation of the cipher
- 7- Consider the Affine cipher with a plaintext space consisting (sequentially) of the English alphabet (small case letters) and three characters: space (), Question mark (?) and exclamation mark (!).
- What is the modulus (n) to be used in the encryption? Justify your answer.
 - Consider the value (a) as the first non-zero digit of your ID (starting with the least significant digit and moving to the left), and (b) as the next digit to the left. Example: for an ID equal 11900120, the value of (a) will be two and that of (b) is one.
 - Explain why the value of a and b are valid
 - Encrypt your first name using the affine cipher with the values of a, b and n .
 - Write the decryption equation. Explain your answer.
- 8- Ali and Bilal decide to use affine cipher to secure their exchanged messages. A message might consist of any letter (capital and small) of the alphabet (a-z, A-Z), any number (0-9) in addition to the comma (,), period (.) and space () characters. Recall that in the affine cipher, a message x is encrypted as $y = ax + b$, where (a, b) is the encryption key.
- What should be the value of n ? Justify your answer
 - What is the size of the key space (i.e., the valid combinations of (a, b))?
 - Ali and Bilal decided to use $(7, 5)$ as their encryption key. Explain why their choice is valid. T
 - Ali wants to send the message “hello” to Bilal using the key of part c). What will be the ciphertext?
 - Explain how Bilal will decrypt the received ciphertext. Detail your answer by explaining the decryption function used by Bilal to decrypt.
 - Eva intercepted the ciphertext sent by Ali. She has a very old computer that can test only one key per second. What is the maximum time it would take for Eva to find the message, assuming that all keys are equiprobable?
- 9- Consider an affine cipher $E(x) = ax + b \bmod n$ where $a = 3, b = 6$ and $n = 26$.
- Explain why the choice of a and b is valid
 - Encrypt your family name using this cipher
- 10- Consider an affine cipher $E(x) = a * x + b \pmod{26}$ which encrypts “H” as “X” and “Q” as “Y”. Find (a, b) .
- 11- Consider an affine cipher with the encryption function: $f(x) = (28x + 49) \bmod 79$. Determine the corresponding decryption function $f^{-1}(x)$.



Playfair Cipher

- 12- Using Playfair cipher, decrypt the following ciphertext ECURSCFTVA given that the keyword for encryption is security
- 13- Encrypt the following message “uluniversity” using Playfair cipher and your last name as a key.
- 14- Encrypt the following message “encryptthis” using Playfair cipher and your last name as a key
- 15- Encrypt the word “strictness” with Playfair cipher using your **last name** as a key. You can use the letter ‘x’ as filler letter if needed
- 16- Decrypt the ciphertext “GPNXOCFHTE” knowing that it was encrypted using PLAYFAIR cipher with “CYBERSECURITY” as a secret key, with ‘X’ as a filler letter.
- 17- Decrypt the following ciphertext (RPVLMNNGSICLFN) encrypted with the Playfair Cipher using the password “PLAYFAIR”

Hill Cipher

- 18- The following ciphertext (DNPRCX) has been encrypted using Hill Cipher. The encryption matrix is

$$K = \begin{bmatrix} 5 & -3 \\ -3 & 2 \end{bmatrix}$$

- a. Verify that the inverse matrix K^{-1} is $\begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$
- b. Decrypt the ciphertext to find the corresponding plaintext
- 19- You are trying to find the encryption key for a Hill cipher with block size two for a regular alphabet size of 26 and know that the plaintext "TRIP" maps to the ciphertext "TJMP". Use this information to determine the encryption key. Note: The encryption key is a matrix of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $0 \leq a, b, c, d \leq 25$.

Vigenère Cipher

- 20- Decrypt the ciphertext WCGHEWMVDFDS knowing it was encrypted using Vigenère Cipher with the key “crypto”. Detail your answer

- 21- Consider the following ciphertext encrypted with Vigenère cipher:

VPXZGIXIVWPUBTTMJPWIZITWZT

Find the plaintext knowing the key used for encryption was **CIPHER**

- 22- Consider the Vigenère Cipher with a plaintext space consisting of the English alphabet (small case letters), the space character and the ten digits (0-9). The characters values are assigned sequentially starting with a (value 0) and ending with the digit 9.
- a. What is the modulus to be used in the encryption process? Justify your answer.
- b. Encrypt your first and last name (separated by space) using your university ID as a key.
- c. What is the size of the key space if you consider that the maximum message size is equal to the length of your first name and last name (separated by space)? Justify your answer



- 23- Consider the following ciphertext that is encrypted using Vigenère cipher. Explain how you might guess the key length. Note that the spaces are not part of the ciphertext but they are just added for the readability of the ciphertext.

KLRWT CSHWD RDBLH NOWIZ IJZKS XJGDX XWSLA BXUAG CILBG VDNOW EBXKS PLJLN QMIGL
ZEJYK IXAYZ ENFYJ WCLEAR SOAVW PWFZY LADZD ABKQC LEARHB RDMZB GYUIA SWMVA RGDSM

- 24- Decrypt the ciphertext WJYABGNZITACOV knowing it was encrypted using Vigenère Cipher with the key “crypto”. Detail your answer

- 25- The following text has been encrypted using a Vigenère key of length 3:

ZHYW IQBO SUPJ DNXX

You have reason to believe that the plaintext starts with *What*. Decrypt it.

Transposition Ciphers

- 26- Encrypt your first, middle and last names (concatenated together) using RAILFENCE transposition cipher. Detail your answer
- 27- Decrypt the following ciphertext “RHAX TNUX REDE AIER IKAT SOQR” given that it has been encrypted using a row-column transposition cipher where the encryption key is : 6 5 3 1 2 4

Additional Exercises

- 28- The adversary has intercepted the following plaintext-ciphertext pair (known-plaintext attack), and wants to find out the key. However, the adversary is not sure which cipher was used (violating Kirchhoff’s principle):

Plaintext M:	c	r	y	p	t	a	n	a	l	y	s	i	s
Ciphertext C:	y	v	y	z	p	e	n	k	h	c	s	s	o

- Which cipher was used for encryption (Transposition, Caesar, Vigenère, Hill $n = 2, \dots$)?
 - Determine the key used for encryption.
- 29- Alice and Bob decided to use a double encryption algorithm that combines substitution and permutation operations in order to secure their communication. They use a random substitution cipher (table below), followed by a row-column transposition cipher with the following key: 2 5 4 3 1. They use ‘z’ as a filler letter.

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	
Y	W	X	Z	F	N	Q	L	S	H	I	E	O	V	R		J	C	A	B	U	P	T	M	K	G	D

- Encrypt the message “cryptography is fun”
- Suppose that Eve intercepted the ciphertext message. How many attempts she has to do in order to break the cipher.
- 30- Consider the Vernam Cipher. Given the message $M = \mathbf{1001101}$ and using the key $K = \mathbf{1010101}$, find the ciphertext? Explain how to get the plaintext (how to decrypt)?