Affine Ciphers

Affine Cipher

- Input/output: $\{a, b, \ldots, z\}$ with encoding $\{0, 1, \ldots, 25\}$
- Encryption: $E(x) = \alpha\, x + \beta \pmod{26}$ such that $\gcd(\alpha, 26) = 1$
- Decryption: $D(y) = \gamma\, y + \theta \pmod{26}$
  such that $\gamma = \alpha^{-1} \pmod{26}$ and $\theta = -\alpha^{-1}\beta \pmod{26}$
- The encryption key: (α, β) with restriction that $\gcd(\alpha, 26) = 1$
  The decryption key: (γ, θ) as given above
- Since 26 is divisible by 2 and 13, we have 12 possible α or γ values:
  $\alpha \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$
  However, there are 26 β values: $\beta \in \{0, 1, \ldots, 25\}$
- The key space size $12 \times 26 = 312$

Affine Cipher

- For $(\alpha, \beta) = (15, 10)$, "hello" is encrypted as "lsttm" since
  $E(\texttt{"h"}) = E(7) = 15 \cdot 7 + 10 = 115 = 11 \pmod{26} \rightarrow \texttt{"l"}$
  $E(\texttt{"e"}) = E(4) = 15 \cdot 4 + 10 = 70 = 18 \pmod{26} \rightarrow \texttt{"s"}$
  $E(\texttt{"l"}) = E(11) = 15 \cdot 11 + 10 = 175 = 19 \pmod{26} \rightarrow \texttt{"t"}$
  $E(\texttt{"o"}) = E(14) = 15 \cdot 14 + 10 = 220 = 12 \pmod{26} \rightarrow \texttt{"m"}$
- Since $(\alpha, \beta) = (15, 10)$, we obtain
  $\gamma = 15^{-1} \ = \ 7 \pmod{26}$
  $\theta = -15^{-1} \cdot 10 \ = \ -7 \cdot 10 \ = \ 8 \bmod 26$
- For $(\gamma, \theta) = (7, 8)$, "lsttm" is decrypted as "hello" since
  $D(\texttt{"l"}) = D(11) = 7 \cdot 11 + 8 = 85 = 7 \pmod{26} \rightarrow \texttt{"h"}$
  $D(\texttt{"s"}) = D(18) = 7 \cdot 18 + 8 = 134 = 4 \pmod{26} \rightarrow \texttt{"e"}$
  $D(\texttt{"t"}) = D(19) = 7 \cdot 19 + 8 = 141 = 11 \pmod{26} \rightarrow \texttt{"l"}$
  $D(\texttt{"m"}) = D(12) = 7 \cdot 12 + 8 = 92 = 14 \pmod{26} \rightarrow \texttt{"o"}$

Exhaustive Key Search

- Given an encrypted text: `"ufqfau omf fndo vnee"`, decrypt the text exhaustively all possible keys:

$\xrightarrow{(1,1)}$ `"tepezt nle emcn umdd"`

$\xrightarrow{(1,2)}$ `"sdodys mkd dlbm tlcc"`

...

$\xrightarrow{(11,12)}$ `"wxyxgw max xtlm ptee"`

$\xrightarrow{(11,13)}$ `"defend the east wall"`

- Similar to the Shift Cipher, a short encrypted text may have several meaningful decryptions, however, for a sufficiently long encrypted text, there will not be ambiguity
- Since there 312 are possible keys, we will have to do 312 decryptions; we may also have to check whether each decrypted text is meaningful

Frequency Analysis

- The previous short ciphertext: `"ufqfau omf fndo vnee"` suggests that `"f"` (most probably) is the ciphertext for the letter `"e"`, and thus,

$$\begin{aligned} D(\texttt{"f"}) &= \texttt{"e"} \\ \gamma \cdot 5 + \theta &= 4 \pmod{26} \end{aligned}$$

This is a linear equation with two unknowns; it can be solved by:

1. Exhaustively enumerating γ values (there are 12 of them), and solving θ from the above equation, and decrypting the text using (γ, θ), and finally, checking to see if a meaningful message is obtained — therefore, performing only 12 decryptions instead of 312
2. Obtaining another plaintext and ciphertext pair, and thus, 2 linear equations with 2 unknowns which can be solved using Gaussian elimination

Frequency Analysis

- The ciphertext `"ufqfau omf fndo vnee"` shows that the second most frequently occurring letters are `"n"`, `"o"`, `"u"`, and `"e"` are the ciphertext of the letters `"t"` and `"a"` — but we cannot be sure which is which
- Let's assume `"n"` is the encryption of `"t"`, this implies

$$\begin{aligned} D(\texttt{"n"}) &= \texttt{"t"} \\ \gamma \cdot 13 + \theta &= 19 \pmod{26} \end{aligned}$$

Together with the previous equation, we have

$$\begin{aligned} \gamma \cdot 5 + \beta &= 4 \pmod{26} \\ \gamma \cdot 13 + \beta &= 19 \pmod{26} \end{aligned}$$

Solving Linear Equations in Modular Arithmetic

- Apply Gaussian elimination (or any other matrix method) but always perform arithmetic mod 26
- Important: if at any point we need the inversion of a number, the number needs to be relatively prime to 26 for inverse to exist
- By elimination, we obtain $8 \cdot \gamma = 15 \pmod{26}$ from the above two equations, however, this equation cannot be solved to find a unique γ since 8 is not invertible mod 26 because $\gcd(8, 26) \neq 1$
- Therefore, our assumption "n" is the encryption of "t" was not correct

Frequency Analysis

- Now, let's assume, "o" is the encryption of "t", we obtain

$$\begin{aligned} D(\texttt{"o"}) &= \texttt{"t"} \\ \gamma \cdot 14 + \theta &= 19 \pmod{26} \end{aligned}$$

- Therefore, we now have the linear equations

$$\begin{aligned} \gamma \cdot 5 + \theta &= 4 \pmod{26} \\ \gamma \cdot 14 + \theta &= 19 \pmod{26} \end{aligned}$$

- By elimination we obtain $9 \cdot \gamma = 15 \pmod{26}$

Frequency Analysis

- This equation is solvable to give a unique γ since $\gcd(9, 26) = 1$

$$\gamma = 9^{-1} \cdot 15 = 3 \cdot 15 = 45 = 19 \pmod{26}$$

- Furthermore, we find θ as

$$\theta = 4 - 5 \cdot \gamma = 4 - 5 \cdot 19 = -91 = 13 \pmod{26}$$

- Therefore, we find $(\gamma, \theta) = (19, 13)$
- If we decrypt the encrypted message using $(\gamma, \theta) = (19, 13)$, we get

$$\texttt{"ufqfau omf fndo vnee"} \xrightarrow{(19,13)} \texttt{"defend the east wall"}$$

Known and Chosen Text Scenarios

- If we have two legitimate (correct) pairs of plaintext and ciphertext (x_1, y_1) and (x_2, y_2), whether are given or chosen, we can write two sets of linear equations modulo 26 as

$$\begin{aligned} \gamma \cdot y_1 + \theta &= x_1 \pmod{26} \\ \gamma \cdot y_2 + \theta &= x_2 \pmod{26} \end{aligned}$$

  and solve it using Gaussian elimination and mod 26 arithmetic to obtain the decryption keys (γ, θ)
- Of course, we may not know a priori that these pairs are correct; however, if they are not correct, the decrypted text will not be meaningful
- If we have more pairs, we can verify the decryption keys on them before decrypting a long text

Cryptanalysis of Affine Cipher

- The Affine Cipher is only slightly stronger than the Shift Cipher
- The number of keys is larger than the Shift Cipher: 312 versus 26
- It requires 2 known (or chosen) pairs of plaintext and ciphertext to break
- The Shift and Affine Cipher are **mono-alphabetic** ciphers which means the same plaintext letter is always mapped to the same ciphertext letter, regardless of its location in the plaintext
- If we want more security, we should consider a **poly-alphabetic** cipher which maps the same plaintext letter to different letters; Examples: Hill Cipher and Vigenère Cipher, and Affine Block Ciphers

Hill Cipher

- Same encoding as the Shift and Affine Ciphers:
  $\{a, b, \ldots, z\} \longrightarrow \{0, 1, \ldots, 25\}$
- Select a $d \times d$ matrix $\mathcal{A}$ of integers and find its inverse $\mathcal{A}^{-1}$ mod 26
- For example, for $d = 2$

$$\mathcal{A} = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \quad \text{and} \quad \mathcal{A}^{-1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

Verify

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} = \begin{bmatrix} 105 & 78 \\ 130 & 79 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{26}$$

Hill Cipher

- Encryption function: $v = \mathcal{A}\, u \pmod{26}$ such that u and v are $d \times 1$ vectors of plaintext and ciphertext letter encodings
- Decryption function: $u = \mathcal{A}^{-1}\, v \pmod{26}$
- Encryption key $\mathcal{A}$: a $d \times d$ matrix such that $\det(\mathcal{A}) \neq 0 \pmod{26}$
- Decryption key $\mathcal{A}^{-1}$: a $d \times d$ matrix which is the inverse of $\mathcal{A}$ mod 26
- Key space: Number of $d \times d$ invertible matrices mod 26

A 2-Dimensional Hill Cipher Example

- The plaintext: "help"

$$u_1 = \begin{bmatrix} \texttt{"h"} \\ \texttt{"e"} \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix} \; ; \quad u_2 = \begin{bmatrix} \texttt{"l"} \\ \texttt{"p"} \end{bmatrix} = \begin{bmatrix} 11 \\ 15 \end{bmatrix}$$

- Encryption: $v_1 = \mathcal{A}\, u_1$ and $v_2 = \mathcal{A}\, u_2$

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 33 \\ 34 \end{bmatrix} = \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} \texttt{"h"} \\ \texttt{"i"} \end{bmatrix}$$

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 11 \\ 15 \end{bmatrix} = \begin{bmatrix} 78 \\ 97 \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} \texttt{"a"} \\ \texttt{"t"} \end{bmatrix}$$

The ciphertext: "hiat"

Hill Cipher

- To decrypt the ciphertext: `"hiat"`, we need the vectors v_1 and v_2
- Decryption: $u_1 = \mathcal{A}^{-1} v_1$ and $u_2 = \mathcal{A}^{-1} v_2$

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 241 \\ 212 \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} \texttt{"h"} \\ \texttt{"e"} \end{bmatrix}$$

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} 323 \\ 171 \end{bmatrix} = \begin{bmatrix} 11 \\ 15 \end{bmatrix} = \begin{bmatrix} \texttt{"l"} \\ \texttt{"p"} \end{bmatrix}$$

The plaintext: `"help"`

- The d-dimensional Hill cipher is poly-alphabetic on single letters, however, mono-alphabetic on words of length d

Key Space Size for Hill Space

- It was suggested by Overbey, Traves, and Wojdylo in *Cryptologia*, 29(1), Jan 2005, that the number of $d \times d$ matrices invertible modulo m is

$$\prod_i \left(p_i^{(n_i-1)d^2} \prod_{k=0}^{d-1} (p_i^d - p_i^k) \right)$$

  such that $m = \prod p_i^{n_i}$

- When $m = 26 = 2^1 \cdot 13^1$, we simplify this as

$$\prod_{k=0}^{d-1} (2^d - 2^k)(13^d - 13^k) \;=\; 26^{d^2}\,(1-1/2)\cdots(1-1/2^d)(1-1/13)\cdots(1-1/13^d)$$

Key Space Size for Hill Cipher

- We enumerate and find the number of keys for as follows:

d	Number of Keys	Decimal	Binary
2	157,248	$10^{5.2}$	$2^{17.3}$
3	1,750,755,202,560	$10^{12.2}$	$2^{40.7}$
4	13,621,827,326,505,327,820,800	$10^{22.1}$	$2^{75.5}$
5	72,803,944,226,174,990,390,435,243,910,758,400	$10^{34.9}$	$2^{115.8}$

- Exhaustive key search is probably not feasible for 4-dimensional Hill ciphers (requires significant resources), and definitely not feasible for 5-dimensional (and beyond) Hill ciphers

A Special Hill Cipher

- Lester Hill (the author of Hill cipher) suggested that an involutory matrix can be used as the Hill matrix
- An involutory matrix is the inverse of itself: $\mathcal{A}^2 = I$
- This way, the encryption and decryption keys are the same:
  Encryption function: $v = \mathcal{A}\, u \pmod{26}$
  Decryption function: $u = \mathcal{A}\, v \pmod{26}$
- This would be good to have from the implementation point of view: we will have to design a single code (or circuit) implementing both the encryption and decryption functions — we do not need to compute the inverse of $\mathcal{A}$

Frequency Analysis of the Hill Cipher

- Frequency analysis is not applicable for single letters — a plaintext letter is encrypted to different ciphertext letter depending on whether it is the first or second letter and what the other letter is
- For example, for our example 2-dimensional Hill cipher, the encryption of x is as follows:

  "xy" → "lk" implies "x" → "l"

  "xz" → "op" implies "x" → "o"

  "zx" → "oj" implies "x" → "j"
- However, digrams (2-letter words) are always encrypted to the same ciphertext bigrams for a 2-dimensional cipher

  "xyabcd" → "lkdfpt"

  "abxycd" → "dflkpt"

  "abcdxy" → "dfptlk"

Digram Frequencies in English

Order and Frequency of Leading DIGRAMS

TH	3.15%	TO	1.11%	SA	0.75%	MA	0.56%
HE	2.51	NT	1.10	HI	0.72	TA	0.56
AN	1.72	ED	1.07	LE	0.72	CE	0.55
IN	1.69	IS	1.06	SO	0.71	IC	0.55
ER	1.54	AR	1.01	AS	0.67	LL	0.55
RE	1.48	OU	0.96	NO	0.65	NA	0.54
ES	1.45	TE	0.94	NE	0.64	RO	0.54
ON	1.45	OF	0.94	EC	0.64	OT	0.53
EA	1.31	IT	0.88	IO	0.63	TT	0.53
TI	1.28	HA	0.84	RT	0.63	VE	0.53
AT	1.24	SE	0.84	CO	0.59	NS	0.51
ST	1.21	ET	0.80	BE	0.58	UR	0.49
EN	1.20	AL	0.77	DI	0.57	ME	0.48
ND	1.18	RI	0.77	LI	0.57	WH	0.48
OR	1.13	NG	0.75	RA	0.57	LY	0.47

Frequency Analysis of the Hill Cipher

- We can apply frequency attack to a d-dimensional Hill cipher if we have “useful” (distinguishable) d-gram frequencies
- As expected the digram `"th"` appears in English more often — some studies have shown that the frequency of diagram `"th"` is about 3.15%
- Similarly the frequency of `"the"` is higher than most other trigrams, followed up by `"and"`, `"for"` — however, these frequencies are too low and too close to one another
- As expected, as the word size increases the frequencies become indistinguishable from one another — we loose those useful frequency values such as 12.7% for the single letter `"e"`

Known or Chosen Text Analysis

- The Hill Cipher is easily broken using a small number of known (or chosen) plaintext and ciphertext pairs
- In order to show this, we will formulate the Hill Cipher as an Affine Block Cipher
- It turns out several other poly-alphabetic ciphers also fall into this category — particularly, the Vigenère Cipher can also be modeled as an Affine Block Cipher
- We will show that a d-dimensional Affine Block Cipher can be broken using $d+1$ ciphertext and plaintext vectors which is equivalent to $d(d+1)$ ciphertext and plaintext letters

Input/Output Alphabet and Encoding

- Input/output alphabet is $\{a, b, \ldots, z\}$ with encoding $\{0, 1, \ldots, 25\}$
- However, other encodings can also be used, for example, we can increase the input size by adding capital letters, punctuation symbols, etc
- In general, we will assume that our alphabet consists of m symbols, represented using the integers $\mathcal{Z}_m = \{0, 1, 2, \ldots, m-1\}$
- Furthermore, we will perform the addition and multiplication operations mod m
- The set and the operations together is called *the ring of integers modulo m*, represented as the triple $(\mathcal{Z}_m, +, \times)$

The Affine Block Cipher

- Encryption function:

$$v = \mathcal{A}\, u + w \pmod{m}$$

  such that u and v are $d \times 1$ input (plaintext) and output (ciphertext) vectors, $\mathcal{A}$ is a fixed $d \times d$ key matrix and w is a $d \times 1$ fixed key vector
- Decryption function:

$$u = \mathcal{A}^{-1}\,(v - w) \pmod{m}$$

  such that $\mathcal{A}^{-1}$ is the inverse of $\mathcal{A}$ in the ring $(\mathcal{Z}_m, +, \times)$
- All elements of these vectors and matrices are from $\mathcal{Z}_m$ and the arithmetic is performed in the ring $(\mathcal{Z}_m, +, \times)$, i.e., modulo m arithmetic

The Affine Block Cipher

- Encryption keys: $\mathcal{A}$ and w
- Decryption keys: $\mathcal{A}^{-1}$ and w
- Key space: The number of distinct invertible $\mathcal{A}$ matrices times the number of distinct w vectors
- Observation: The Hill Cipher is an Affine Block Cipher such that $\mathcal{A}$ is the Hill matrix, w is a zero vector, and $m = 26$

$$\begin{aligned} v &= \mathcal{A}\, u \pmod{26} \\ u &= \mathcal{A}^{-1}\, v \pmod{26} \end{aligned}$$

The Vigenère Cipher

- Another well known cipher is the Vigenère Cipher which was incorrectly attributed to Blaise de Vigenère (1523-1596), a French diplomat and cryptographer
- It seems that the Vigenère Cipher was reinvented several times!
- The Vigenère Cipher makes use of repeated applications of the Shift Cipher with different keys — it is a poly-alphabetic cipher
- The Vigenère Cipher is easy to understand and implement, and seems unbreakable to beginners, which explains its popularity!
- It has earned a special name: *le chiffre indéchiffrable*

The Vigenère Cipher - Informal Description

- Select a key word or key phrase: `herbalist`
- Write key word under the plaintext message and perform mod 26 addition on letter encodings in order to obtain the plaintext

```
physicists at ucsb are studying quantum entanglement
herbalisth er bali sth erbalist herbali stherbalisth
wlptinqkmz ek vcdj skl wkvdjqfz xyrotfu wgaeehlpuwga
```

- For example, to find "p" + "h" we add their encodings 15 and 7 modulo 26, and thus

$$15 + 7 = 22 \pmod{26}$$

obtain 22 which is the encoding of "w"

The Vigenère Cipher - Affine Block Cipher

- The key word length (in our example $d = 9$) is the dimension of the Affine Block Cipher representing the Vigenère Cipher
- The key word itself is represented as $d \times 1$ vector with elements from $\mathcal{Z}_{26}$
- In our example, `herbalist` implies $w = [7, 4, 17, 1, 0, 11, 8, 18, 19]^T$
- The encryption function is given simply as $v = u + w \pmod{26}$ where u and v are the plaintext and ciphertext vectors of dimension 9×1
- In other words, the Vigenère Cipher is an Affine Block Cipher with $\mathcal{A} = I$, the unit matrix, that is $v = \mathcal{A}v + w = v + w \pmod{26}$
- The decryption function is obtained as $u = v - w \pmod{26}$

The Vigenère Cipher - Affine Block Cipher

- As an example, let us obtain the encryption of the plaintext "physicist" which is encoded as $u = [15, 7, 24, 18, 8, 2, 8, 18, 19]^T$
- Since $w = [7, 4, 17, 1, 0, 11, 9, 18, 19]^T$, we obtain the ciphertext

$$v = u + w = \begin{bmatrix} 15 \\ 7 \\ 24 \\ 18 \\ 8 \\ 2 \\ 8 \\ 18 \\ 19 \end{bmatrix} + \begin{bmatrix} 7 \\ 4 \\ 17 \\ 1 \\ 0 \\ 11 \\ 8 \\ 18 \\ 19 \end{bmatrix} = \begin{bmatrix} 22 \\ 11 \\ 15 \\ 19 \\ 8 \\ 13 \\ 17 \\ 10 \\ 12 \end{bmatrix} = \begin{bmatrix} \texttt{"w"} \\ \texttt{"l"} \\ \texttt{"p"} \\ \texttt{"t"} \\ \texttt{"i"} \\ \texttt{"n"} \\ \texttt{"q"} \\ \texttt{"k"} \\ \texttt{"m"} \end{bmatrix}$$

Known (or Chosen) Text Analysis

- Now we show how to obtain the key ($\mathcal{A}$ and w) of an Affine Block Cipher using a set of known or chosen texts
- Consider the encryption function of the d-dimensional Affine Block Cipher:

$$v = \mathcal{A}\, u + w \pmod{m}$$

  such that u, v, w are $d \times 1$ vectors and $\mathcal{A}$ is a $d \times d$ matrix
- Assume that we have $d + 1$ pairs of (known or chosen) plaintext and ciphertext vectors:

$$(u_i, v_i) \quad \text{for} \quad i = 0, 1, 2, \ldots, d$$

- Since each vector has d elements, this means we have $d(d + 1)$ plaintext and ciphertext letters

Known (or Chosen) Text Analysis

- This means each pair (u_i, v_i) satisfies the equation

$$v_i = \mathcal{A}\, u_i + w \pmod{m}$$

for $i = 0, 1, 2, \ldots, d$, and particularly, $v_0 = \mathcal{A}\, u_0 + w \pmod{m}$

- This implies

$$\begin{aligned} v_i - v_0 &= \mathcal{A}\, u_i + w - (\mathcal{A}\, u_0 + w) \pmod{m} \\ &= \mathcal{A}\, u_i - \mathcal{A}\, u_0 \pmod{m} \\ &= \mathcal{A}(u_i - u_0) \pmod{m} \end{aligned}$$

where the vector $(u_i - u_0)$ is of dimension $d \times 1$

Known (or Chosen) Text Analysis

- Assemble the $d \times 1$ column vectors $(u_i - u_0)$ and $(v_i - v_0)$ into respective matrices of dimension $d \times d$ as

$$\begin{aligned} \mathcal{U} &= [u_1 - u_0,\ u_2 - u_0,\ u_3 - u_0,\ \cdots,\ u_d - u_0] \\ \mathcal{V} &= [v_1 - v_0,\ v_2 - v_0,\ v_3 - v_0,\ \cdots,\ v_d - v_0] \end{aligned}$$

- This way we can write all d equations as follows:

$$\mathcal{V} = \mathcal{A}\mathcal{U} \pmod{m}$$

- By finding the inverse of the $d \times d$ matrix $\mathcal{U}$, and multiplying both sides of the above equation, we find

$$\mathcal{A} = \mathcal{V}\mathcal{U}^{-1} \pmod{m}$$

Known (or Chosen) Text Analysis

- Once we have the key matrix $\mathcal{A}$, we easily obtain the key vector w as

$$w = v_0 - \mathcal{A}\, u_0 \pmod{m}$$

- This analysis requires $d + 1$ knows plaintext and ciphertext vectors: (u_i, v_i) for $i = 0, 1, 2, \ldots, d$ — since each vector has d entries, we need $d(d + 1)$ plaintext and ciphertext letters
- Considering that d is the dimension of the system, and is probably a small integer, this attack is very powerful
- For example, the 5-dimensional Hill cipher had $10^{115.8}$ keys, making the exhaustive key search an impossible task — however, we can break it using only $5 \cdot 6 = 30$ plaintext and ciphertext pairs