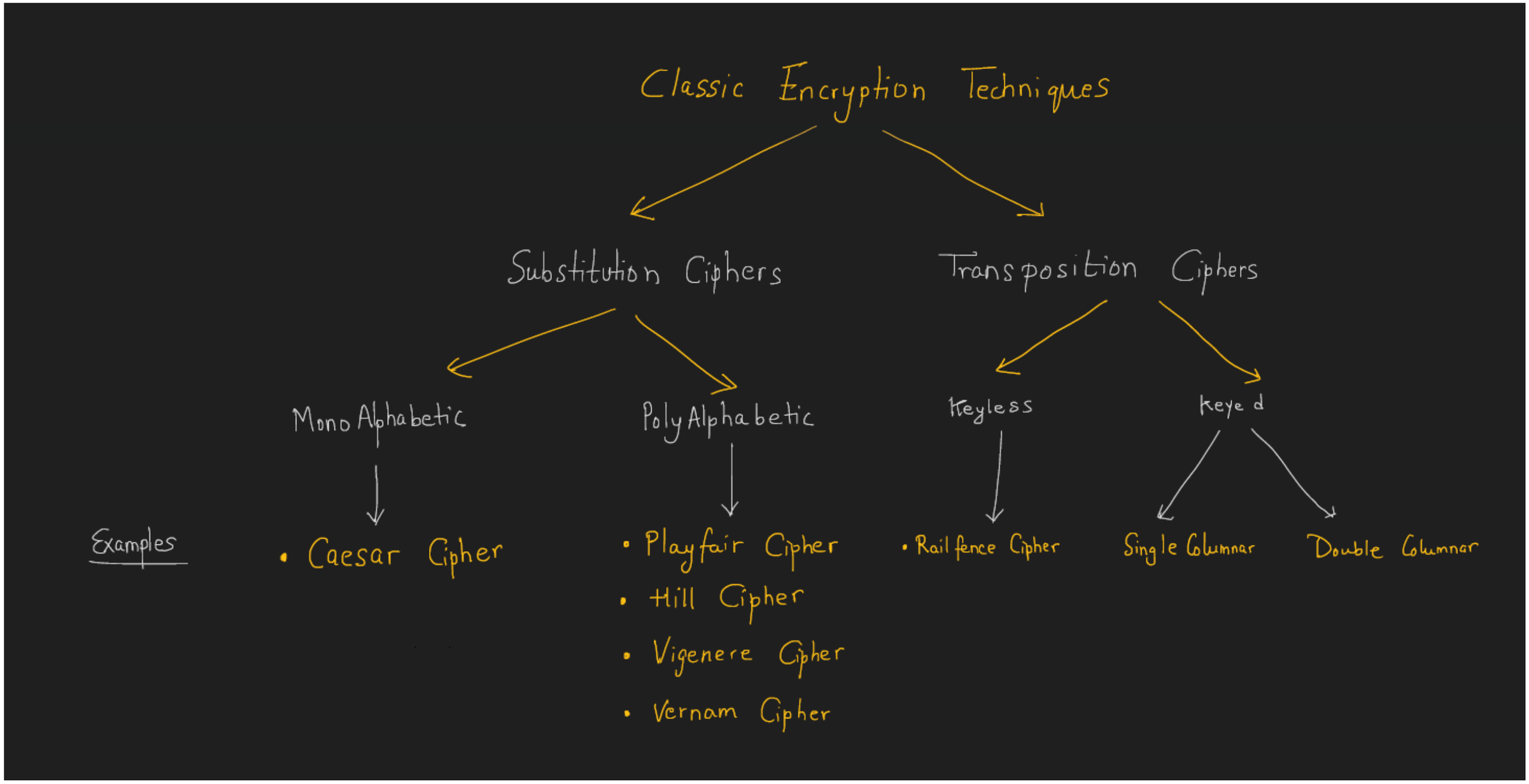
Module 1: Introduction and Number Theory

Caesar Cipher and Playfair Cipher



Substitution Cipher

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

1. Caesar Cipher

The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example,

```
plain:  meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB
```

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows:

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

Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Then the algorithm can be expressed as follows. For each plaintext letter p, substitute the ciphertext letter C

$$C = \mathrm{E}(3, p) = (p + 3) \bmod 26$$

A shift may be of any amount, so that the general Caesar algorithm is

$$C = \mathrm{E}(k, p) = (p + k) \bmod 26$$

where k takes on a value in the range 1 to 25. The decryption algorithm is simply

$$p = \mathrm{D}(k, C) = (C - k) \bmod 26$$

If it is known that a given ciphertext is derived using a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys. The image below shows the results of applying this strategy to the example ciphertext. In this case, the plaintext leaps out as occupying the third line.

Three important characteristics of this problem enabled us to use a bruteforce cryptanalysis:
1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.

```
          PHHW PH DIWHU WKH WRJD SDUWB
KEY
  1       oggv og chvgt vjg vqic rctva
  2       nffu nf bgufs uif uphb qbsuz
  3       meet me after the toga party
  4       ldds ld zesdq sgd snfz ozqsx
  5       kccr kc ydrcp rfc rmey nyprw
  6       jbbq jb xcqbo qeb qldx mxoqv
  7       iaap ia wbpan pda pkcw lwnpu
  8       hzzo hz vaozm ocz ojbv kvmot
  9       gyyn gy uznyl nby niau julns
 10       fxxm fx tymxk max mhzt itkmr
 11       ewwl ew sxlwj lzw lgys hsjlq
 12       dvvk dv rwkvi kyv kfxr grikp
 13       cuuj cu qvjuh jxu jewq fqhjo
 14       btti bt puitg iwt idvp epgin
 15       assh as othsf hvs hcuo dofhm
 16       zrrg zr nsgre gur gbtn cnegl
 17       yqqf yq mrfqd ftq fasm bmdfk
 18       xppe xp lqepc esp ezrl alcej
 19       wood wo kpdob dro dyqk zkbdi
 20       vnnc vn jocna cqn cxpj yjach
 21       ummb um inbmz bpm bwoi xizbg
 22       tlla tl hmaly aol avnh whyaf
 23       skkz sk glzkx znk zumg vgxze
 24       rjjy rj fkyjw ymj ytlf ufwyd
 25       qiix qi ejxiv xli xske tevxc
```

Some Exercises on Caesar Cipher

Decrypt the following using Standard Caesar Cipher (Key - 3)

1. Vxevwlwxwlrq Flskhu

2. Fubswrjudskb lv lqwhuhvwlqj

3. Zh pdnh d vkliw ri wkuhh lq wklv flskhu

Decrypt the following (Key not given, Brute Force)

1. Jpapglu

2. Wxikerskvetlc

3. Pcvkqpcnkva

2. Playfair Cipher

The Playfair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword.

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

In this case, the keyword is monarchy. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter. Plaintext is encrypted two letters at a time, according to the following rules:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.

2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.

3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.

4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

Example

Plaintext: Instruments

Key : Monarchy

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

Step 1: Make Pairs of the Plaintext Characters

IN ST RU ME NT SX

Step 2: Follow algo. steps 1 to 4 to convert the plaintext pairs into ciphertext pairs.

For eg IN ⇒ GA , ST ⇒ TL

RU ⇒ MZ , ME ⇒ CL

NT ⇒ RQ , SX ⇒ XA

Step 3: Write Down the final Ciphertext.

CT ⇒ GA TLMZ CLRQXA

Some Exercises on Playfair Cipher

Q. Encrypt the following using Playfair Cipher

1. Plaintext ⇒ Cryptography

   Keyword ⇒ Nation

2. Plaintext ⇒ Universal College

   Keyword ⇒ Engineering

3. Plaintext ⇒ This is Playfair Cipher

   Keyword ⇒ Networks