Data Attacks:

An attempted crypto analysis is known as an attack. The level of information that decoder is able to extract from the cryptosystem and can be divided into five ways of decryption which are as follows:

Cipher text only attack: The crypto analyst has cipher text of several messages and all of which were encrypted using the same encryption algorithm. Then job is to recover the plain text or the key used to encrypt the messages. So, to decrypt other part of messages encrypted with the help of same keys.

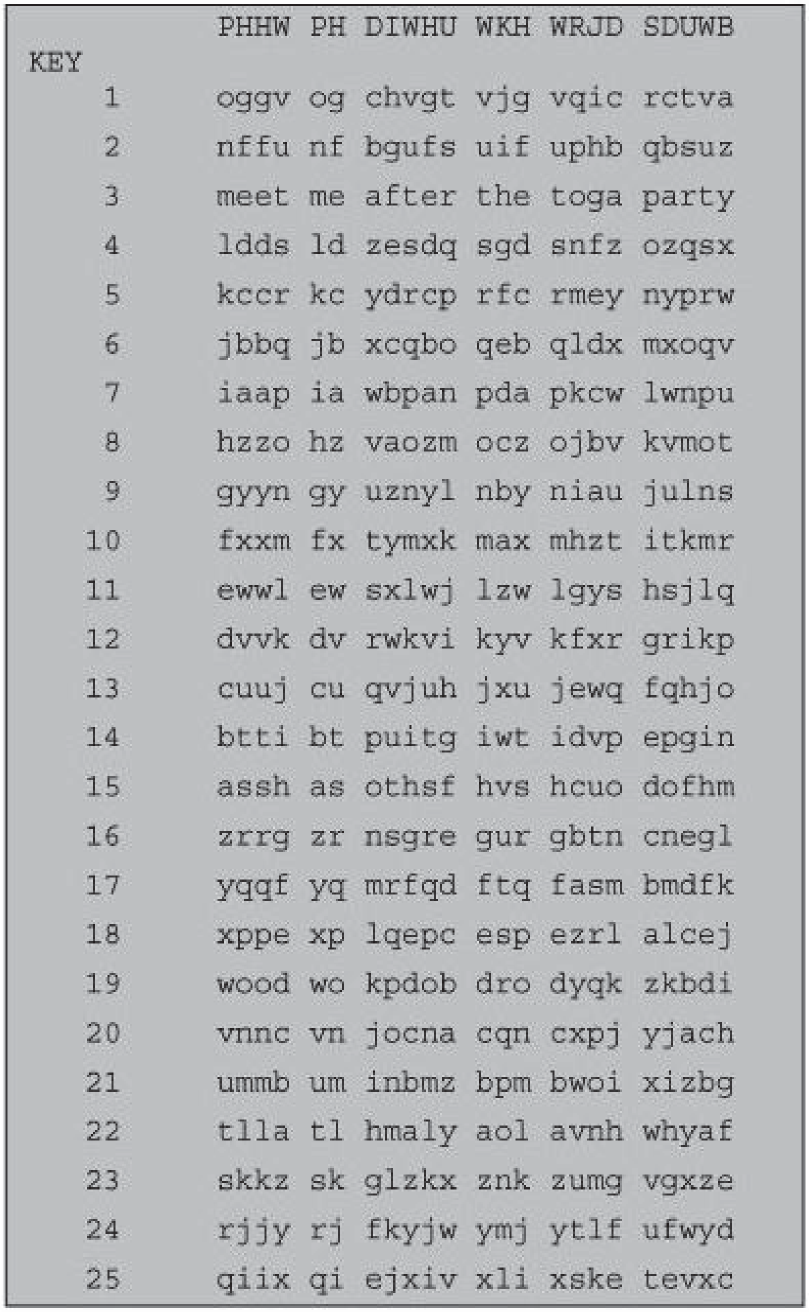
Known Plaintext attack: Crypto analysts seek the possession of pairs of known plain text and cipher text. Then job is to hold the key used to encrypt the messages or an algorithm to decrypt messages.

Chosen Plaintext Attack (CPA): Crypto analyst not only hold the cipher text but also some parts of chosen plain text. Intruder is identified to be placed at encryption site to do the attack.

Chosen cipher text attack (CCA): In this crypto analyst hold the possession of chosen cipher text and plain text being decrypted from the private key. However, it only has access to an encryption machine.

Cryptanalysis of Caesar Cipher

If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed. A brute-force attack involves systematically checking all possible keys until the correct key is found. Simply try all the 25 possible keys. In this case, the plaintext leaps out as occupying the third line.



KEY	PHHW PH DIWHU WKH WRJD SDUWB
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

Three important characteristics of this problem enabled us to use a brute-force 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.