LAB – 1 Classic Ciphers

B00122875 Vimal Jaswal

The origins of modern cryptography date back approximately 3000 years. The procedures used to encrypt messages before 1900 were primitive compared to modern approaches, but they are easy to understand and provide a good basis to study the more complicated methods. In recent times, especially after the emergence of telecommunication equipment, more complex encryption methods have become necessary. Today, an exorbitant amount of information is transmitted via the internet. Millions of people use websites for their banking activities causing the transmission of sensible data via networks where the precise routing of data is not always known, and data may be manipulated or stolen.

This lab will use the tools on the http://www.cryptool-online.org/ website to give you the opportunity to learn about ciphers and to test them in an interactive way within your browser. Try to encrypt a message for yourself and send it to a friend. Learn about the weak spots of popular ciphers and how they can be decrypted without knowing the key.

Exercise 1: Rotational ciphers (substitution or shift Ciphers)

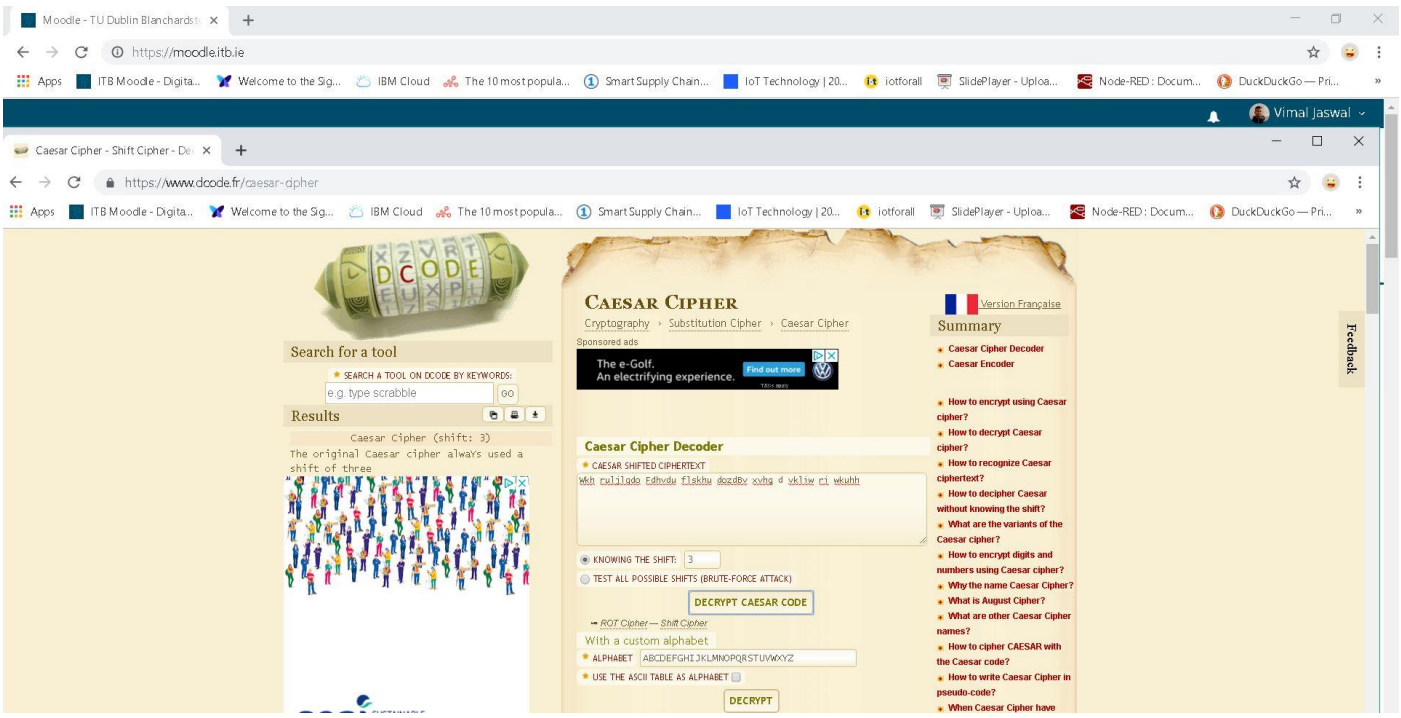
One of the classic ciphers I'm sure we've all seen as magazine puzzles etc. is the **Caesar Cipher**. It's essential a simplified substitution Cipher, that shifts each letter in the alphabet 3 characters A>D, B>E etc. The idea has been extended many times to allow a different shift amount (the key) so it's not always 3. One common variation is called **Rot-13** which allows us to use the same function for encryption and decryption.

Using the extra information and examples from the Cryptool website study these classic ciphers and answer the following questions.

Decode this classic Caesar's ciphers:

a. Wkh ruljlqdo Fdhvdu flskhu dozdBv xvhg d vkliw ri wkuhh

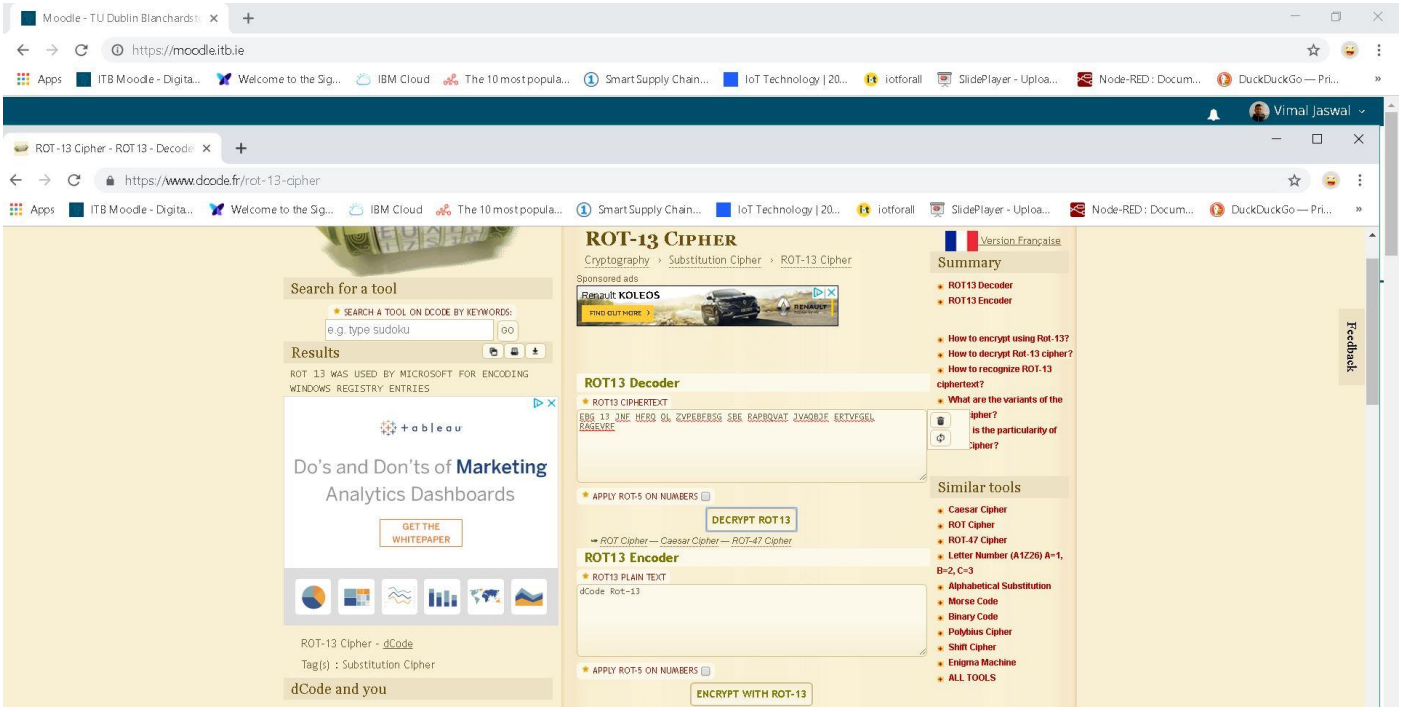
The original Caesar cipher alwaYs used a shift of three



Decode this ROT-13 cipher:

b. EBG 13 JNF HFRQ OL ZVPEBFBSG SBE RAPBQVAT JVAQBJF ERTVFGEL RAGEVRF

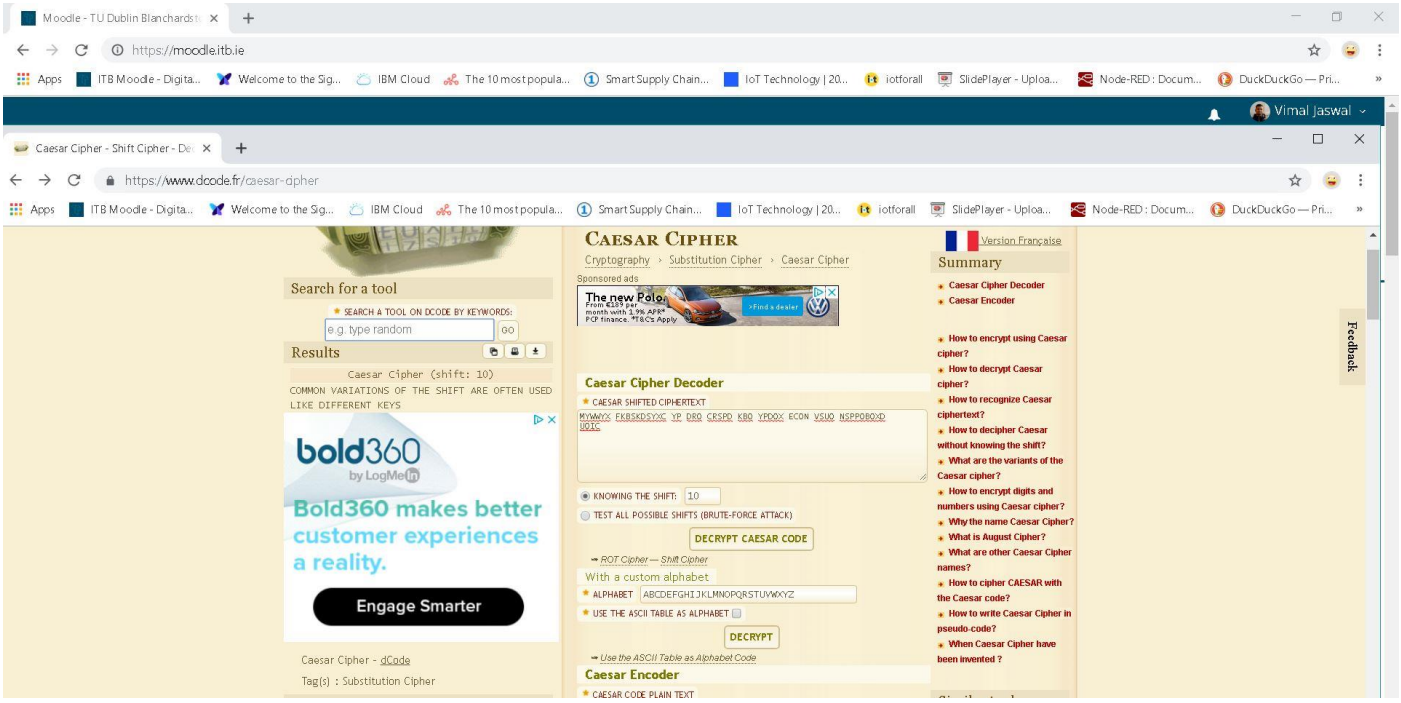
ROT 13 WAS USED BY MICROSOFT FOR ENCODING WINDOWS REGISTRY ENTRIES



Try decode the following messages that have all been encoded using shift ciphers.

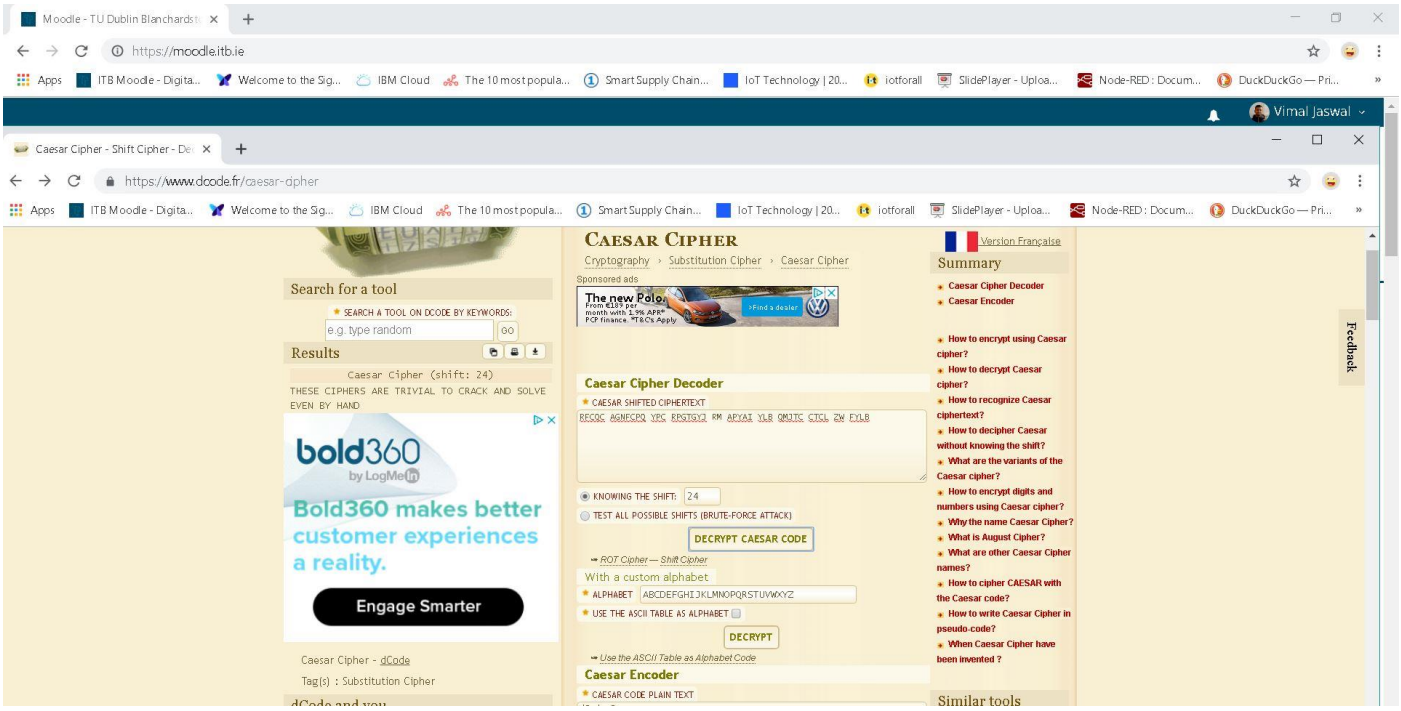
c. MYWWYX FKBSKDSYXC YP DRO CRSPD KBO YPDOX ECON VSUO NSPPOBOXD UOIC

COMMON VARIATIONS OF THE SHIFT ARE OFTEN USED LIKE DIFFERENT KEYS



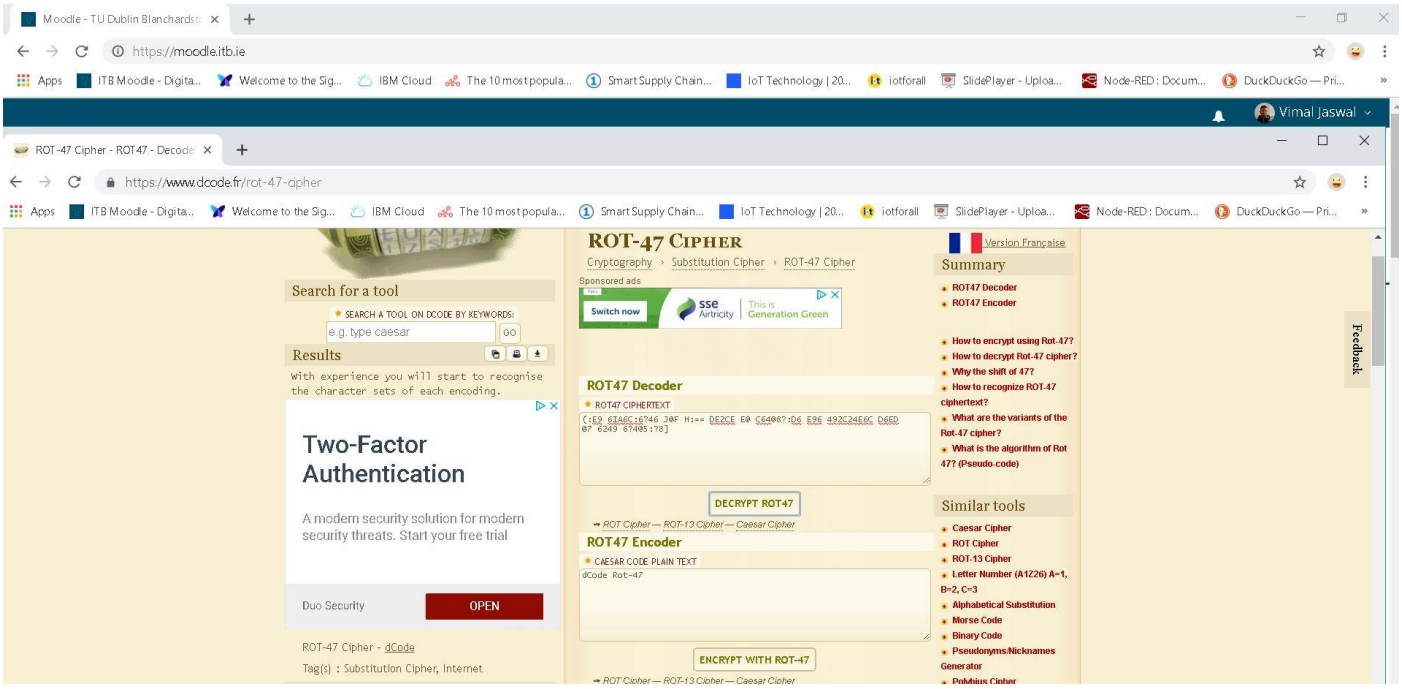
d. RFCQC AGNFCPQ YPC RPGTGYJ RM APYAI YLB QMJTC CTCL ZW FYLB

THESE CIPHERS ARE TRIVIAL TO CRACK AND SOLVE EVEN BY HAND



e. (:E9 6IA6C:6?46 J@F H:== DE2CE E@ C64@8?:D6 E96 492C24E6C D6ED @7 6249 6?4@5:?8]

With experience you will start to recognise the character sets of each encoding.



Exercise 2: Substitution Ciphers

Rotational or shift ciphers are very easy to crack and decode. An improvement on this type of encoding that became very popular and much more difficult to break became the substitution cipher. Essentially each letter was mapped to a different letter in the alphabet. The more encrypted text we had the easier it became to decode these ciphers but very short messages are extremely difficult.

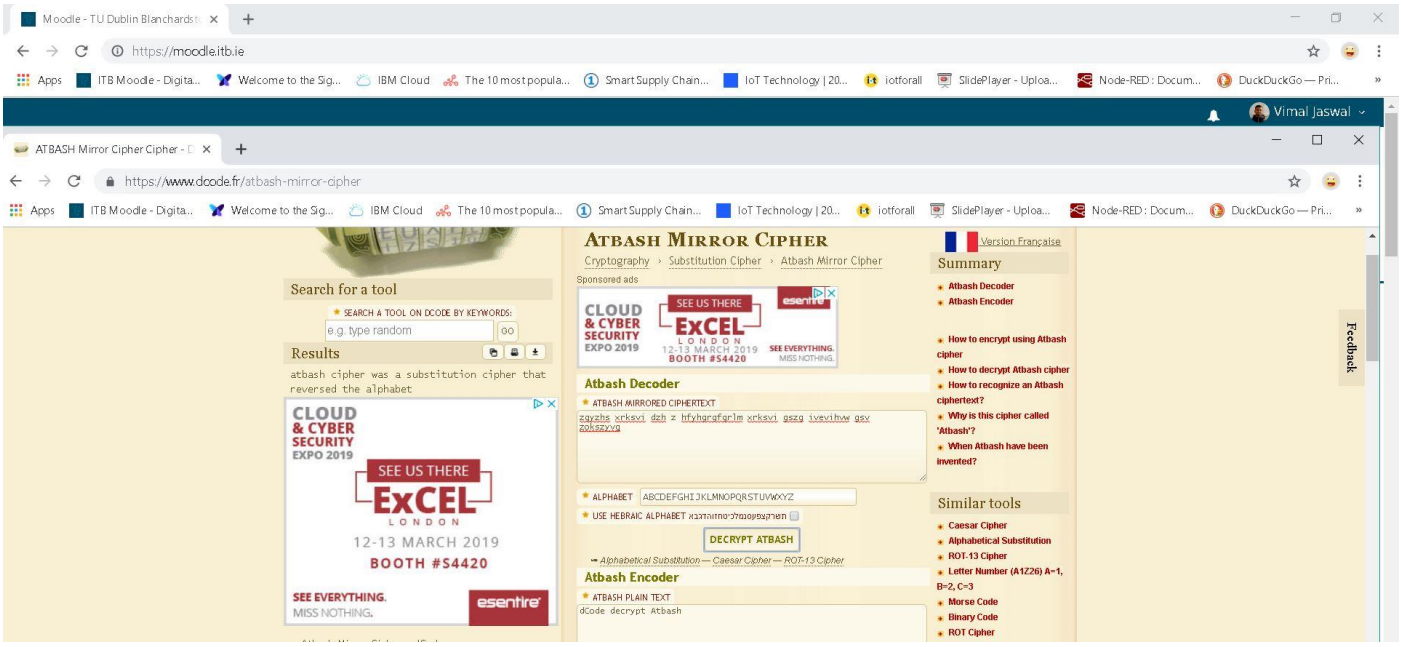
Decoder rings became popular between groups, armies and even lovers. (Do a quick google on decoder rings for more.)

Some of the simplest forms of monoalphabetic ciphers included the **Atbash** cipher, which basically just reversed the alphabets, so A>Z, B>Y etc. and also the **Kamasutra Cipher, Playfair** and **Multiplicative Cipher**.

These were improved to randomise the pairings between letters and the key effectively became the entire mapping. Later variations of these ciphers mapped the original alphabet to different symbols and pairs of letter combinations to make the decoding harder. (**Alberti Cipher, Pollux Cipher)**
The weakness with these ciphers was exposed using frequency analysis, by count the occurrences of each letter in a cipher text we could match it to it's likely matching plaintext letter. Tables with Frequency analysis details for cryptanalysis details to appear in the 9th century.
Try decoding some of these ciphertexts.

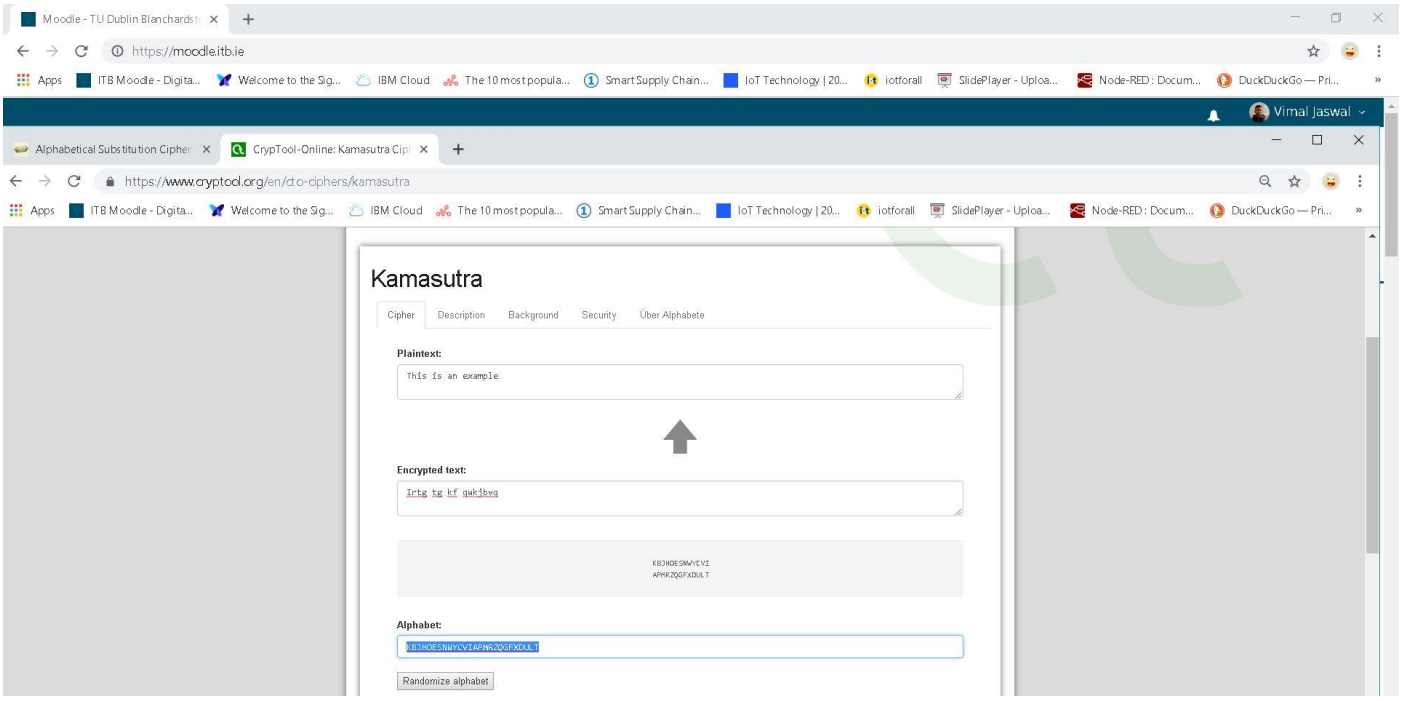
a. **Atbash:** zgyzhs xrksvi dzh z hfyhgrgfgrlm xrksvi gszg ivevihvw gsv zokszyvg

atbash cipher was a substitution cipher that reversed the alphabet



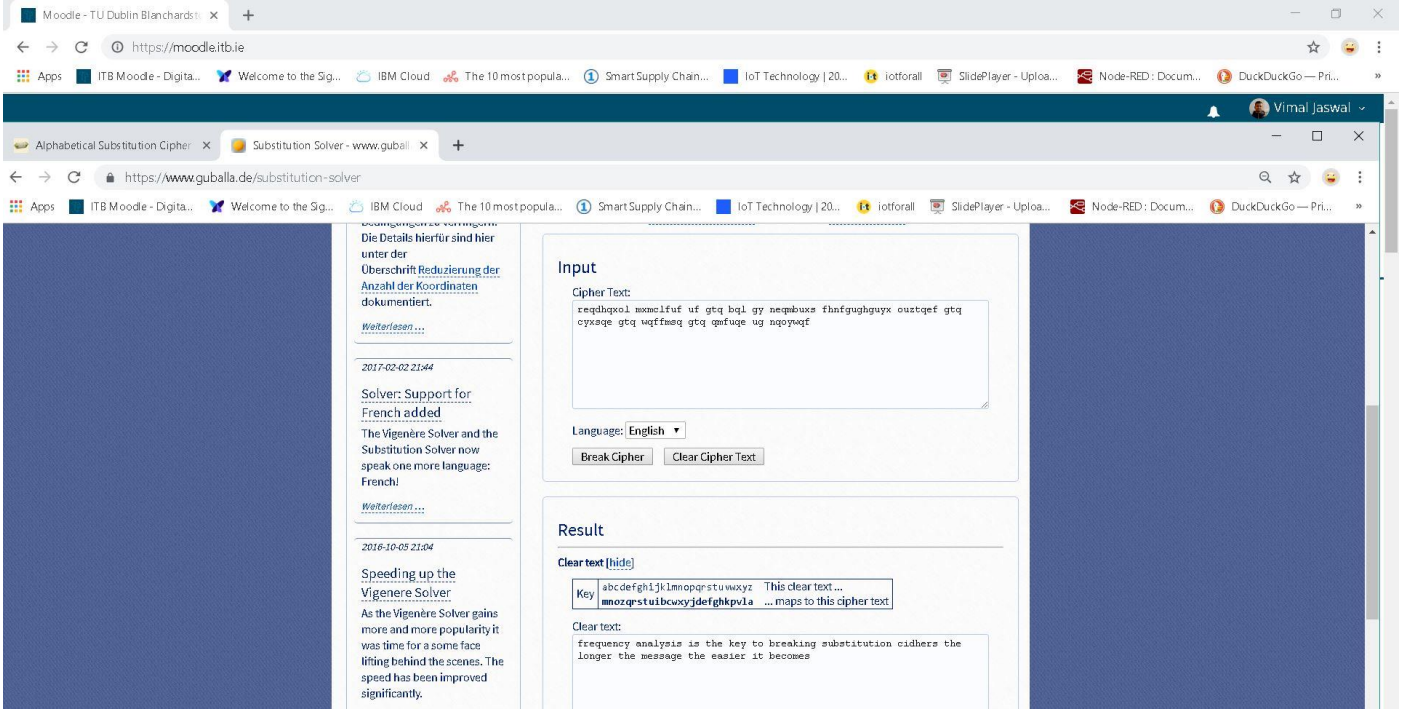
b. **Kamasutra:** Irtg tg kf qwkjbvq
Upper half: KBJHOESNWYCVI
Lower half: APMRZQGFXDULT

This is an example



c. reqdhqxol mxmclfuf uf gtq bql gy neqmbuxs fhnfgughguyx ouztqef gtq cyxsqe gtq wqffmsq gtq qmfuqe ug nqoywqf

frequency analysis is the key to breaking substitution ciphers the longer the message the easier it becomes

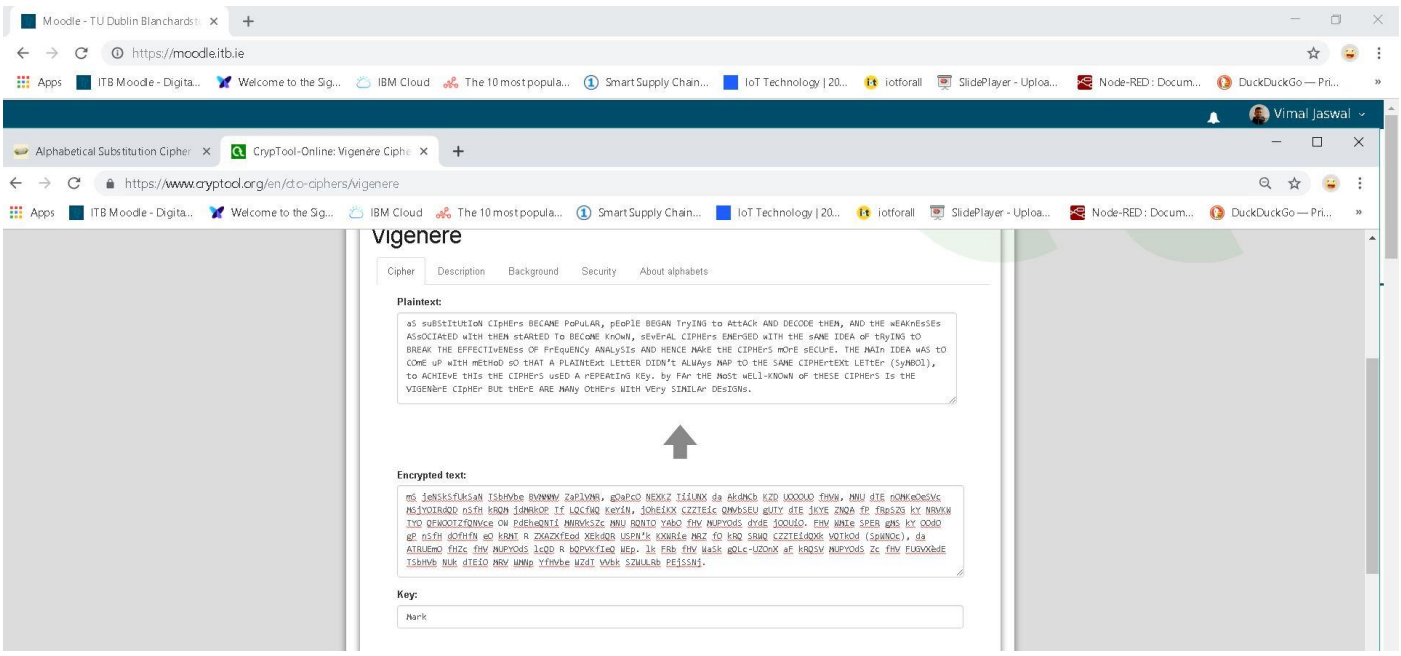


Exercise 3:
As substitution ciphers became popular, people began trying to attack and decode them, and the weaknesses associated with them started to become known, several ciphers emerged with the same idea of trying to break the effectiveness of frequency analysis and hence make the ciphers more secure. The main idea was to come up with method so that a plaintext letter didn't always map to the same ciphertext letter (symbol), to achieve this the ciphers used a repeating key. By far the most well-known of these ciphers is the **Vigenère cipher** but there are many others with very similar designs. **(Autokey, Beaufort, Gronsfeld, Larrabee, Trithemius, Porta, Polybius)**

Try decode this Vigenère cipher:

mS jeNSkSfUkSaN TSbHVbe BVMMMV ZaPlVMR, gOaPcO NEXKZ TiiUNX da AkdMCb KZD UOOOUO fHVW, MNU dTE nOMKeOeSVc MSjYOIRdQD nSfH kRQM jdMRkOP Tf LQCfWQ KeYiN, jOhEiKX CZZTEic QMVbSEU gUTY dTE jKYE ZNQA fP fRpSZG kY NRVKW TYO QFWOOTZfQNVce OW PdEheQNTi MNRVkSZc MNU RQNTO YAbO fHV MUPYOdS dYdE jOOUiO. FHV WMIe SPER gMS kY OOdO gP nSfH dOfHfN eO kRMT R ZXAZXfEod XEkdQR USPN'k KXWRie MRZ fO kRQ SRWQ CZZTEidQXk VQTkOd (SpWNOc), da ATRUEmO fHZc fHV MUPYOdS lcQD R bQPVKfIeQ WEp. lk FRb fHV WaSk gQLc-UZOnX aF kRQSV MUPYOdS Zc fHV FUGVXèdE TSbHVb NUk dTEiO MRV WMNp YfHVbe WZdT VVbk SZWULRb PEjSSNj.

aS suBStItUtIoN CIpHErs BECAME PoPuLAR, pEoPlE BEGAN TryING to AttACk AND DECODE tHEM, AND tHE wEAKnEsSEs ASsOCIAtED wItH tHEM stARtED To BECoME KnOwN, sEvErAL CIPHErs EMErGED wITH tHE sAME IDEA oF tRyING tO BREAK THE EFFECTIvENEss OF FrEquENCy ANALySIs AND HENCE MAkE tHE CIPHErS mOrE sECUrE. THE MAIn IDEA wAS tO COmE uP wItH mEtHoD sO tHAT A PLAINtExt LEttER DIDN't ALWAys MAP tO tHE SAME CIPHErtEXt LETtEr (SyMBOl), to ACHIEvE tHIs tHE CIPHErS usED A rEPEAtInG KEy. by FAr tHE MoSt wELl-KNOwN oF tHESE CIPHErS Is tHE VIGENèrE CIpHEr BUt tHErE ARE MANy OtHErs WItH VEry SIMILAr DEsIGNs.



Exercise 4:
One other common type of classic chiper **are transposition ciphers**, these ciphers usually involve writeen the message or alphabet out into a grid or array type pattern and then reading the message down column by column, to produce a outputed ciphertext. In these case the output is often an anagram of the original message. Common ciphers in this category include: **AMSCO, ADFG(V)X, Scytale.**

Try decode this transposition cipher:

qnl uktnefslonom srtltgpvannhyem pi btskhalv ocee go boobcii ei aesniri oegehur semanat eiyr h

or

NRAATIOSSPCOTNIRHIEPCSAOLDLAELMLCUORPNESTTMAUSNIIOHEACTEQNUIACTHOHENTGEREDOHFRTOTEETLNSEIRTEAXTAPBLYINCGIGNTAIDRI

ATRANSPOSITIONCIPHERALSOCALLEDCOLUMNSPERMUTATIONISATECHNIQUETOCHANGETHEORDEROFTHELETTERSINATEXTBYPLACINGITINAGIRD