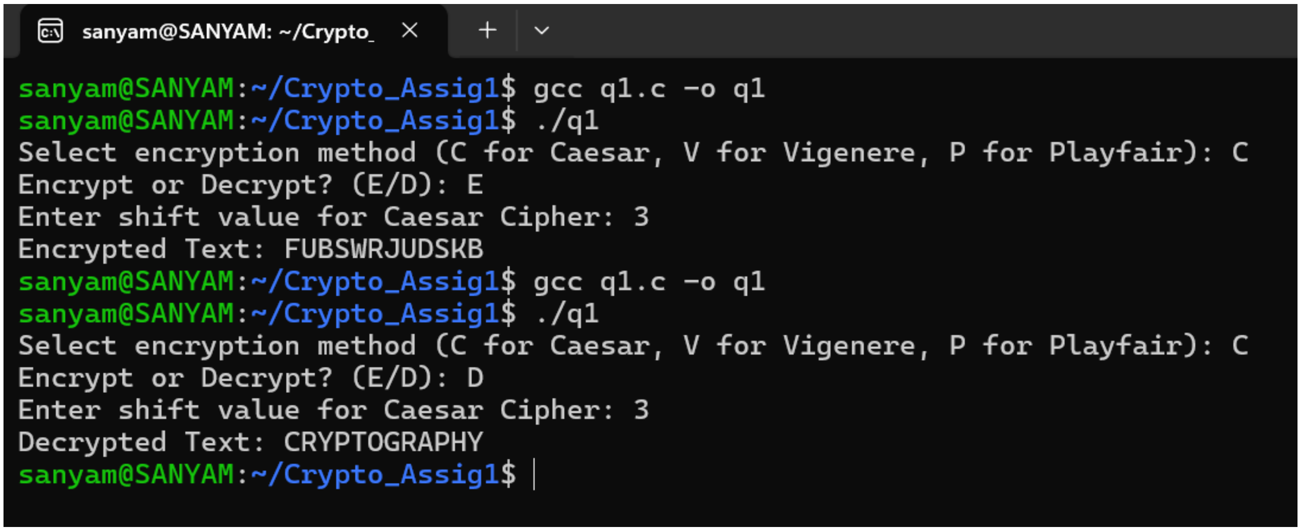
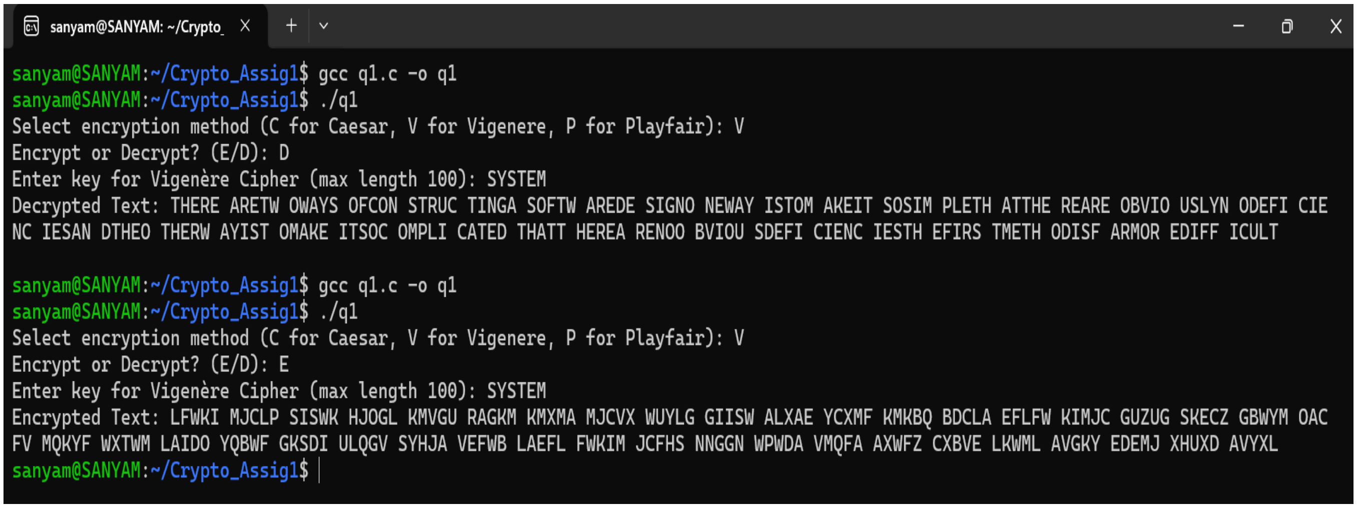
Sanyam Agrawal SE21UCSE192 CSE3

CNS Assignment 1

Q1

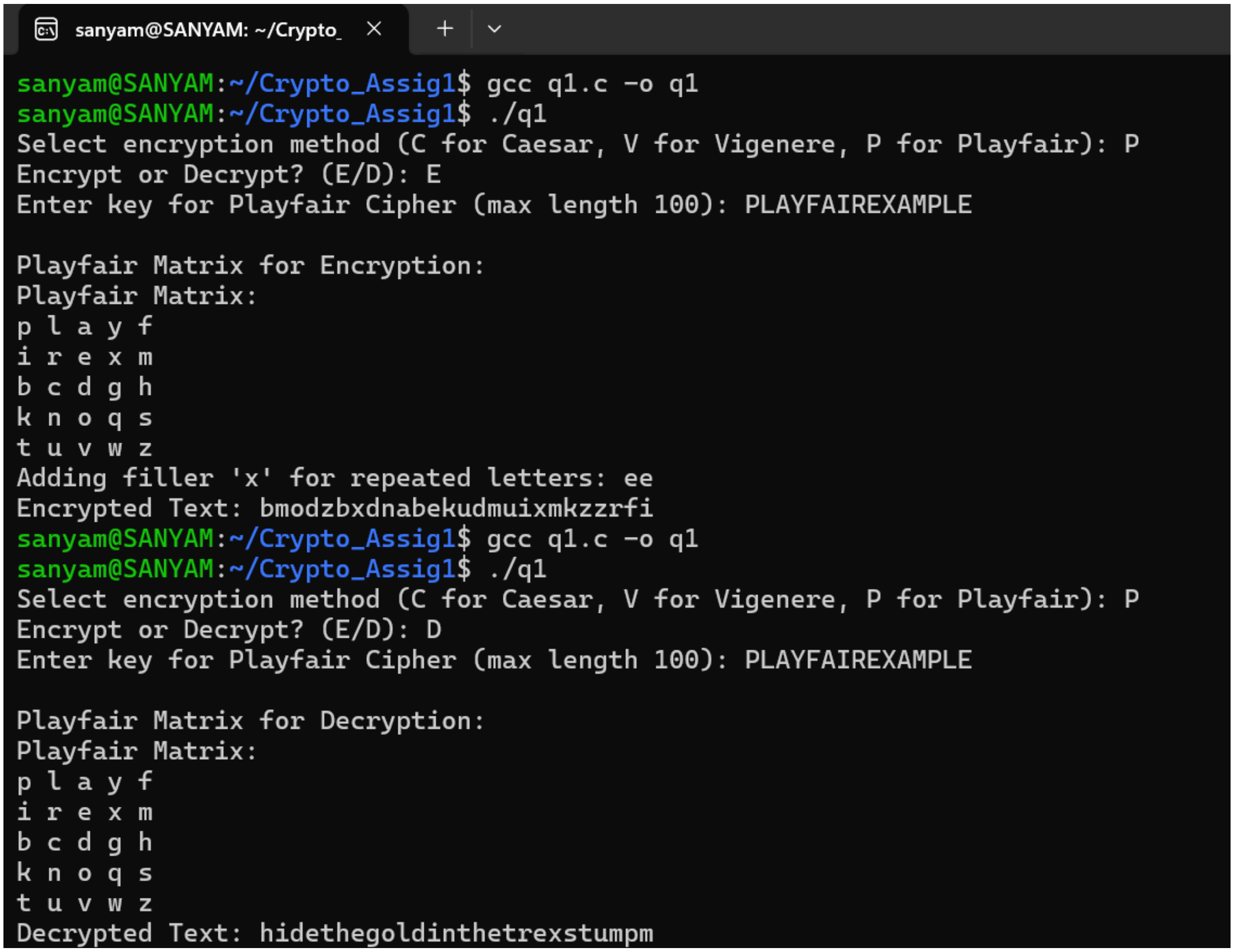


```
sanyam@SANYAM:~/Crypto_Assig1$ gcc q1.c -o q1
sanyam@SANYAM:~/Crypto_Assig1$ ./q1
Select encryption method (C for Caesar, V for Vigenere, P for Playfair): C
Encrypt or Decrypt? (E/D): E
Enter shift value for Caesar Cipher: 3
Encrypted Text: FUBSWRJUDSKB
sanyam@SANYAM:~/Crypto_Assig1$ gcc q1.c -o q1
sanyam@SANYAM:~/Crypto_Assig1$ ./q1
Select encryption method (C for Caesar, V for Vigenere, P for Playfair): C
Encrypt or Decrypt? (E/D): D
Enter shift value for Caesar Cipher: 3
Decrypted Text: CRYPTOGRAPHY
sanyam@SANYAM:~/Crypto_Assig1$ 
```



```
sanyam@SANYAM:~/Crypto_Assig1$ gcc q1.c -o q1
sanyam@SANYAM:~/Crypto_Assig1$ ./q1
Select encryption method (C for Caesar, V for Vigenere, P for Playfair): V
Encrypt or Decrypt? (E/D): D
Enter key for Vigenère Cipher (max length 100): SYSTEM
Decrypted Text: THERE ARETW OWAYS OFCON STRUC TINGA SOFTW AREDE SIGNO NEWAY ISTOM AKEIT SOSIM PLETH ATTHE REARE OBVIO USLYN ODEFI CIE
NC IESAN DTHEO THERW AYIST OMAKE ITSOC OMPLI CATED THATT HEREA RENOO BVIOU SDEFI CIENC IESTH EFIRS TMETH ODISF ARMOR EDIFF ICULT

sanyam@SANYAM:~/Crypto_Assig1$ gcc q1.c -o q1
sanyam@SANYAM:~/Crypto_Assig1$ ./q1
Select encryption method (C for Caesar, V for Vigenere, P for Playfair): V
Encrypt or Decrypt? (E/D): E
Enter key for Vigenère Cipher (max length 100): SYSTEM
Encrypted Text: LFWKI MJCLP SISWK HJOGL KMVGU RAGKM KMXMA MJCVX WUYLG GIISW ALXAE YCXMF KMKBQ BDCLA EFLFW KIMJC GUZUG SKECZ GBWYM OAC
FV MQKYF WXTWM LAIDO YQBWF GKSDI ULQGV SYHJA VEFWB LAEFL FWKIM JCFHS NNGGN WPWDA VMQFA AXWFZ CXBVE LKWML AVGKY EDEMJ XHUXD AVYXL
sanyam@SANYAM:~/Crypto_Assig1$ 
```

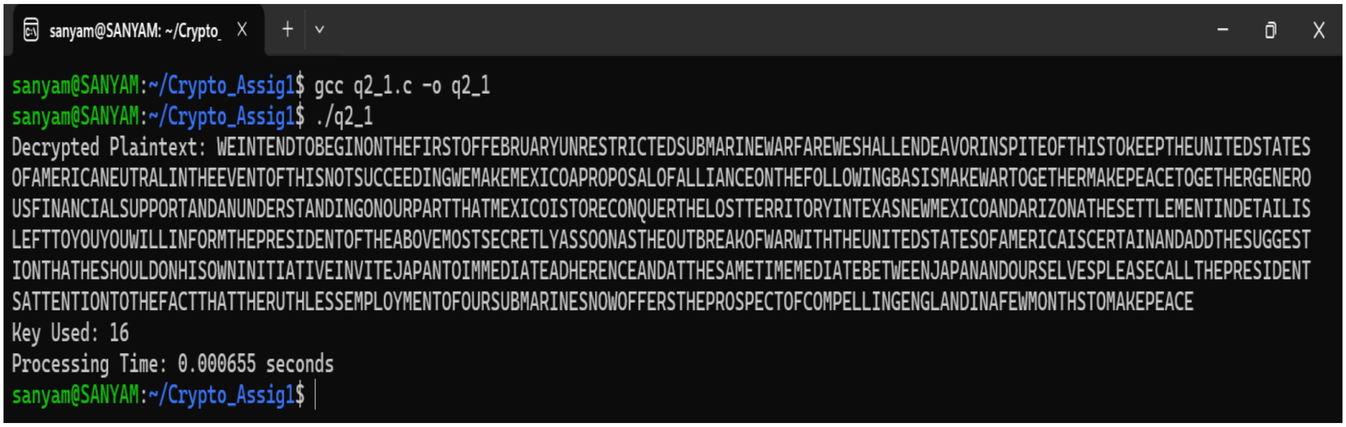


```
sanyam@SANYAM:~/Crypto_Assig1$ gcc q1.c -o q1
sanyam@SANYAM:~/Crypto_Assig1$ ./q1
Select encryption method (C for Caesar, V for Vigenere, P for Playfair): P
Encrypt or Decrypt? (E/D): E
Enter key for Playfair Cipher (max length 100): PLAYFAIREXAMPLE

Playfair Matrix for Encryption:
Playfair Matrix:
p l a y f
i r e x m
b c d g h
k n o q s
t u v w z
Adding filler 'x' for repeated letters: ee
Encrypted Text: bmodzbxdnabekudmuixmkzzrfi
sanyam@SANYAM:~/Crypto_Assig1$ gcc q1.c -o q1
sanyam@SANYAM:~/Crypto_Assig1$ ./q1
Select encryption method (C for Caesar, V for Vigenere, P for Playfair): P
Encrypt or Decrypt? (E/D): D
Enter key for Playfair Cipher (max length 100): PLAYFAIREXAMPLE

Playfair Matrix for Decryption:
Playfair Matrix:
p l a y f
i r e x m
b c d g h
k n o q s
t u v w z
Decrypted Text: hidethegoldinthetrexstumpm
```

Q2.1

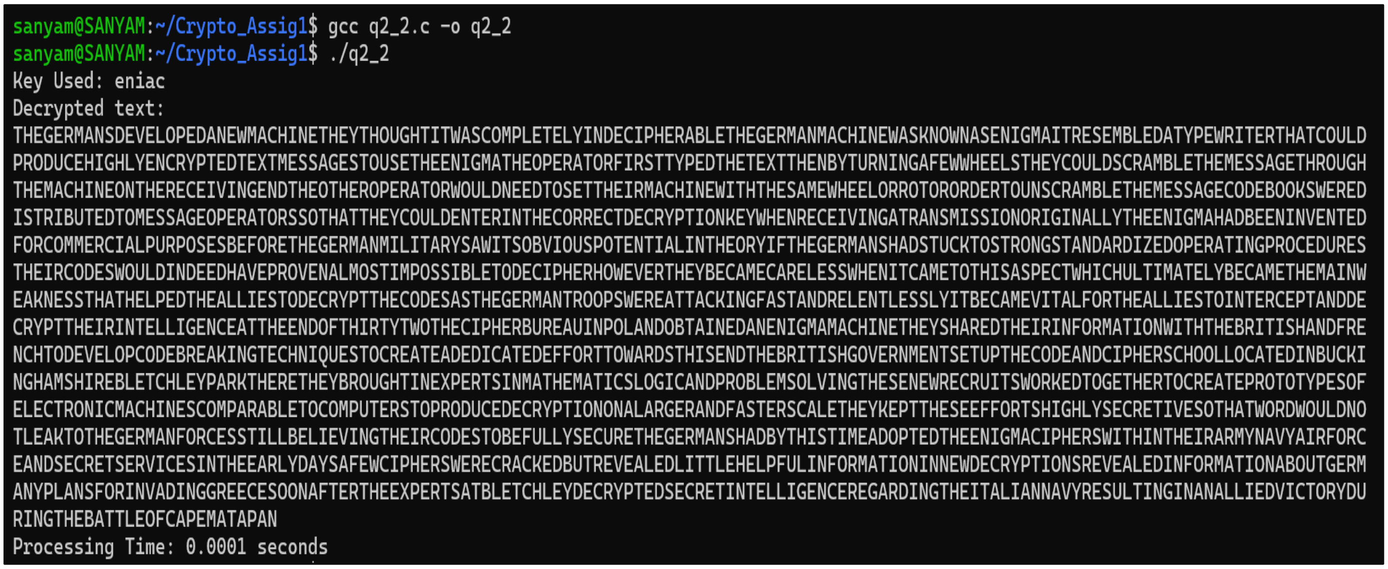


```
sanyam@SANYAM:~/Crypto_Assig1$ gcc q2_1.c -o q2_1
sanyam@SANYAM:~/Crypto_Assig1$ ./q2_1
Decrypted Plaintext: WEINTENDTOBEGINONTHEFIRSTOFFEBRUARYUNRESTRICTEDSUBMARINEWARFAREWESHALLENDEAVORINSPITEOFTHISTOKEEPTHEUNITEDSTATES
OFAMERICANEUTRALINTHEEVENTOFTHISNOTSUCCEEDINGWEMAKEMEXICOAPROPOSALOFALLIANCEONTHEFOLLOWINGBASISMAKEWARTOGETHERMAKEPEACETOGETHERGENERO
USFINANCIALSUPPORTANDANUNDERSTANDINGONOURPARTTHATMEXICOISTORECONQUERTHELOSTTERRITORYINTEXASNEWMEXICOANDARIZONATHESETTLEMENTINDETAILIS
LEFTTOYOUYOUWILLINFORMTHEPRESIDENTOFTHEABOVEMOSTSECRETLYASSOONASTHEOUTBREAKOFWARWITHTHEUNITEDSTATESOFAMERICAISCERTAINANDADDTHESUGGEST
IONTHATHESHOULDONHISOWNINITIATIVEINVITEJAPANTOIMMEDIATEADHERENCEANDATTHESAMETIMEMEDIATEBETWEENJAPANANDOURSELVESPLEASECALLTHEPRESIDENT
SATTENTIONTOTHEFACTTHATTHERUTHLESSEMPLOYMENTOFOURSUBMARINESNOWOFFERSTHEPROSPECTOFCOMPELLINGENGLANDINAFEWMONTHSTOMAKEPEACE
Key Used: 16
Processing Time: 0.000655 seconds
sanyam@SANYAM:~/Crypto_Assig1$
```

Key Used = 16.

WE INTEND TO BEGIN ON THE FIRST OF FEBRUARY UNRESTRICTED SUBMARINE WARFARE WE SHALL ENDEAVOR IN SPITE OF THIS TO KEEP THE UNITED STATES OF AMERICA NEUTRAL IN THE EVENT OF THIS NOT SUCCEEDING WE MAKE MEXICO A PROPOSAL OF ALLIANCE ON THE FOLLOWING BASIS MAKE WAR TOGETHER MAKE PEACE TOGETHER GENEROUS FINANCIAL SUPPORT AND AN UNDERSTANDING ON OUR PART THAT MEXICO IS TO RECONQUER THE LOST TERRITORY IN TEXAS NEW MEXICO AND ARIZONA THE SETTLEMENT IN DETAIL IS LEFT TO YOU YOU WILL INFORM THE PRESIDENT OF THE ABOVE MOST SECRETLY AS SOON AS THE OUTBREAK OF WAR WITH THE UNITED STATES OF AMERICA IS CERTAIN AND ADD THE SUGGESTION THAT HE SHOULD ON HIS OWN INITIATIVE INVITE JAPAN TO IMMEDIATE ADHERENCE AND AT THE SAME TIME MEDIATE BETWEEN JAPAN AND OURSELVES PLEASE CALL THE PRESIDENT'S ATTENTION TO THE FACT THAT THE RUTHLESS EMPLOYMENT OF OUR SUBMARINES NOW OFFERS THE PROSPECT OF COMPELLING ENGLAND IN A FEW MONTHS TO MAKE PEACE

Q2.2



```
sanyam@SANYAM:~/Crypto_Assig1$ gcc q2_2.c -o q2_2
sanyam@SANYAM:~/Crypto_Assig1$ ./q2_2
Key Used: eniac
Decrypted text:
THEGERMANSDEVELOPEDANEWMACHINETHEYTHOUGHTITWASCOMPLETELYINDECIPHERABLETHEGERMANMACHINEWASKNOWNASENIGMAITRESEMBLEDATYPEWRITERTHATCOULD
PRODUCEHIGHLYENCRYPTEDTEXTMESSAGESTOUSETHEENIGMATHEOPERATORFIRSTTYPEDTHETEXTTHENBYTURNINGAFEWWHEELSTHEYCOULDSCRAMBLETHEMESSAGETHROUGH
THEMACHINEONTHERECEIVINGENDTHEOTHEROPERATORWOULDNEEDTOSETTHEIRMACHINEWITHTHESAMEWHEELORROTORORDERTOUNSCRAMBLETHEMESSAGECODEBOOKSWERED
ISTRIBUTEDTOMESSAGEOPERATORSSOTHATTHEYCOULDENTERINTHECORRECTDECRYPTIONKEYWHENRECEIVINGATRANSMISSIONORIGINALLYTHEENIGMAHADBEENINVENTED
FORCOMMERCIALPURPOSESBEFORETHEGERMANMILITARYSAWITSOBVIOUSPOTENTIALINTHEORYIFTHEGERMANSHADSTUCKTOSTRONGSTANDARDIZEDOPERATINGPROCEDURES
THEIRCODESWOULDINDEEDHAVEPROVENALMOSTIMPOSSIBLETODECIPHERHOWEVERTHEYBECAMECARELESSWHENITCAMETOTHISASPECTWHICHULTIMATELYBECAMETHEMAINW
EAKNESSTHATHELPEDTHEALLIESTODECRYPTTHECODESASTHEGERMANTROOPSWEREATTACKINGFASTANDRELENTLESSLYITBECAMEVITALFORTHEALLIESTOINTERCEPTANDDE
CRYPTTHEIRINTELLIGENCEATTHEENDOFTHIRTYTWOTHECIPHERBUREAUINPOLANDOBTAINEDANENIGMAMACHINETHEYSHAREDTHEIRINFORMATIONWITHTHEBRITISHANDFRE
NCHTODEVELOPCODEBREAKINGTECHNIQUESTOCREATEADEDICATEDEFFORTTOWARDSTHISENDTHEBRITISHGOVERNMENTSETUPTHECODEANDCIPHERSCHOOLLOCATEDINBUCKI
NGHAMSHIREBLETCHLEYPARKTHERETHEYBROUGHTINEXPERTSINMATHEMATICSLOGICANDPROBLEMSOLVINGTHESENEWRECRUITSWORKEDTOGETHERTOCREATEPROTOTYPESOF
ELECTRONICMACHINESCOMPARABLETOCOMPUTERSTOPRODUCEDECRYPTIONONALARGERANDFASTERSCALETHEYKEPTTHESEEFFORTSHIGHLYSECRETIVESOTHATWORDWOULDNO
TLEAKTOTHEGERMANFORCESSTILLBELIEVINGTHEIRCODESTOBEFULLYSECURETHEGERMANSHADBYTHISTIMEADOPTEDTHEENIGMACIPHERSWITHINTHEIRARMYNAVYAIRFORC
EANDSECRETSERVICESINTHEEARLYDAYSAFEWCIPHERSWERECRACKEDBUTREVEALEDLITTLEHELPFULINFORMATIONINNEWDECRYPTIONSREVEALEDINFORMATIONABOUTGERM
ANYPLANSFORINVADINGGREECESOONAFTERTHEEXPERTSATBLETCHLEYDECRYPTEDSECRETINTELLIGENCEREGARDINGTHEITALIANNAVYRESULTINGINANALLIEDVICTORYDU
RINGTHEBATTLEOFCAPEMATAPAN
Processing Time: 0.0001 seconds
```

Key Used = **eniac**

THE GERMANS DEVELOPED A NEW MACHINE THEY THOUGHT IT WAS COMPLETELY INDECIPHERABLE THE GERMAN MACHINE WAS KNOWN AS ENIGMA IT RESEMBLED A TYPEWRITER THAT COULD PRODUCE HIGHLY ENCRYPTED TEXT MESSAGES TO USE THE ENIGMA THE OPERATOR FIRST TYPED THE TEXT THEN BY TURNING A FEW WHEELS THEY

COULD SCRAMBLE THE MESSAGE THROUGH THE MACHINE ON THE RECEIVING END THE OTHER OPERATOR WOULD NEED TO SET THEIR MACHINE WITH THE SAME WHEEL OR ROTOR ORDER TO UNSCRAMBLE THE MESSAGE CODEBOOKS WERE DISTRIBUTED TO MESSAGE OPERATORS SO THAT THEY COULD ENTER IN THE CORRECT DECRYPTION KEY WHEN RECEIVING A TRANSMISSION ORIGINALLY THE ENIGMA HAD BEEN INVENTED FOR COMMERCIAL PURPOSES BEFORE THE GERMAN MILITARY SAW ITS OBVIOUS POTENTIAL IN THEORY IF THE GERMANS HAD STUCK TO STRONG STANDARDIZED OPERATING PROCEDURES THEIR CODES WOULD INDEED HAVE PROVEN ALMOST IMPOSSIBLE TO DECRYPT HOWEVER THEY BECAME CARELESS WHEN IT CAME TO THIS ASPECT WHICH ULTIMATELY BECAME THE MAIN WEAKNESS THAT HELPED THE ALLIES TO DECRYPT THE CODES AS THE GERMAN TROOPS WERE ATTACKING FAST AND RELENTLESSLY IT BECAME VITAL FOR THE ALLIES TO INTERCEPT AND DECRYPT THEIR INTELLIGENCE AT THE END OF 1932 THE CIPHER BUREAU IN POLAND OBTAINED AN ENIGMA MACHINE THEY SHARED THEIR INFORMATION WITH THE BRITISH AND FRENCH TO DEVELOP CODE BREAKING TECHNIQUES AND CREATE A DEDICATED EFFORT TOWARDS THIS END THE BRITISH GOVERNMENT SET UP THE CODE AND CIPHER SCHOOL LOCATED IN BUCKINGHAMSHIRE AT BLETCHLEY PARK THERE THEY BROUGHT IN EXPERTS IN MATHEMATICS LOGIC AND PROBLEM SOLVING THESE NEW RECRUITS WORKED TOGETHER TO CREATE PROTOTYPES OF ELECTRONIC MACHINES COMPARABLE TO COMPUTERS TO PRODUCE DECRYPTION ON A LARGER AND FASTER SCALE THEY KEPT THESE EFFORTS HIGHLY SECRETIVE SO THAT WORD WOULD NOT LEAK TO THE GERMAN FORCES STILL BELIEVING THEIR CODES TO BE FULLY SECURE THE GERMANS HAD BY THIS TIME ADOPTED THE ENIGMA CIPHERS WITHIN THEIR ARMY NAVY AIR FORCE AND SECRET SERVICES IN THE EARLY DAYS THE ENIGMA CIPHERS WERE CRACKED BUT REVEALED LITTLE HELPFUL INFORMATION NEW DECRYPTIONS REVEALED INFORMATION ABOUT GERMANY PLANS FOR INVADING GREECE SOON AFTER THE EXPERTS AT BLETCHLEY DECRYPTED SECRET INTELLIGENCE REGARDING THE ITALIAN NAVY RESULTING IN AN ALLIED VICTORY DURING THE BATTLE OF CAPE MATAPAN