Part 1

***Caesar Cipher***

#A python program to illustrate Caesar Cipher Technique  
def encrypt(text,s):  
 result = ""  
  
 # traverse text  
 for i in range(len(text)):  
 char = text[i]  
  
 # Encrypt uppercase characters  
 if (char.isupper()):  
 result += chr((ord(char) + s-65) % 26 + 65)  
  
 # Encrypt lowercase characters  
 else:  
 result += chr((ord(char) + s - 97) % 26 + 97)  
  
 return result  
  
#check the above function  
text = "ATTACKATONCE"  
s = 4  
print("Text : " + text)  
print("Shift : " + str(s))  
print("Cipher: " + encrypt(text,s))  
  
key1 = -3  
cipher
print("Cipher number 1: " + encrypt(cipher1,key1))

***Vigenère Cipher***

# Python code to implement  
# Vigenere Cipher  
  
# This function generates the  
# key in a cyclic manner until  
# it's length isn't equal to  
# the length of original text  
def generateKey(string, key):  
 key = list(key)  
 if len(string) == len(key):  
 return (key)  
 else:  
 for i in range(len(string) -  
 len(key)):  
 key.append(key[i % len(key)])  
 return ("".join(key))  
  
  
# This function returns the  
# encrypted text generated  
# with the help of the key  
def cipherText(string, key):  
 cipher\_text = []  
 for i in range(len(string)):  
 x = (ord(string[i]) +  
 ord(key[i])) % 26  
 x += ord('A')  
 cipher\_text.append(chr(x))  
 return ("".join(cipher\_text))  
  
  
# This function decrypts the  
# encrypted text and returns  
# the original text  
def originalText(cipher\_text, key):  
 orig\_text = []  
 for i in range(len(cipher\_text)):  
 x = (ord(cipher\_text[i]) -  
 ord(key[i]) + 26) % 26  
 x += ord('A')  
 orig\_text.append(chr(x))  
 return ("".join(orig\_text))  
  
  
# Driver code  
if \_\_name\_\_ == "\_\_main\_\_":  
 string = "GEEKSFORGEEKS"  
 keyword = "AYUSH"  
 key = generateKey(string, keyword)  
 cipher\_text = cipherText(string, key)  
 print("Ciphertext :", cipher\_text)  
 print("Original/Decrypted Text :",  
 originalText(cipher\_text, key))  
  
# This code is contributed  
# by Pratik Somwanshi

Part 3

ONEVARIATIONTOTHESTANDARDCAESARCIPHERISWHENTHEALPHABETISKEYEDBYUSINGAWORDINTHETRADITIONALVARIETYONECOULDWRITETHEALPHABETONTWOSTRIPSANDJUSTMATCHUPTHESTRIPSAFTERSLIDINGTHEBOTTOMSTRIPTOTHELEFTORRIGHTTOENCODEYOUWOULDFINDALETTERINTHETOPROWANDSUBSTITUTEITFORTHELETTERINTHEBOTTOMROWFORAKEYEDVERSIONONEWOULDNOTUSEASTANDARDALPHABETBUTWOULDFIRSTWRITEAWORDOMITTINGDUPLICATEDLETTERSANDTHENWRITETHEREMAININGLETTERSOFTHEALPHABETFORTHEEXAMPLEBELOWIUSEDAKEYOFRUMKINCOMANDYOUWILLSEETHATTHEPERIODISREMOVEDBECAUSEITISNOTALETTERYOUWILLALSONOTICETHESECONDMISNOTINCLUDEDBECAUSETHEREWASANMALREADYANDYOUCANTHAVEDUPLICATES

Part 4

Key : 9

ONEVARIATIONTOTHESTANDARDCAESARCIPHERISWHENTHEALPHABETISKEYEDBYUSINGAWORDINTHETRADITIONALVARIETYONECOULDWRITETHEALPHABETONTWOSTRIPSANDJUSTMATCHUPTHESTRIPSAFTERSLIDINGTHEBOTTOMSTRIPTOTHELEFTORRIGHTTOENCODEYOUWOULDFINDALETTERINTHETOPROWANDSUBSTITUTEITFORTHELETTERINTHEBOTTOMROWFORAKEYEDVERSIONONEWOULDNOTUSEASTANDARDALPHABETBUTWOULDFIRSTWRITEAWORDOMITTINGDUPLICATEDLETTERSANDTHENWRITETHEREMAININGLETTERSOFTHEALPHABETFORTHEEXAMPLEBELOWIUSEDAKEYOFRUMKINCOMANDYOUWILLSEETHATTHEPERIODISREMOVEDBECAUSEITISNOTALETTERYOUWILLALSONOTICETHESECONDMISNOTINCLUDEDBECAUSETHEREWASANMALREADYANDYOUCANTHAVEDUPLICATES

Part 5

NIST IS ABOUT TO ANNOUNCE THE NEW HASH ALGORITHM THAT WILL BECOME SHA-3. THIS IS THE RESULT OF A SIX-YEAR COMPETITION, AND MY OWN SKEIN IS ONE OF THE FIVE REMAINING FINALISTS (OUT OF AN INITIAL 64). IT'S PROBABLY TOO LATE FOR ME TO AFFECT THE FINAL DECISION, BUT I AM HOPING FOR "NO AWARD." IT'S NOT THAT THE NEW HASH FUNCTIONS AREN'T ANY GOOD, IT'S THAT WE DON'T REALLY NEED ONE. WHEN WE STARTED THIS PROCESS BACK IN 2006, IT LOOKED AS IF WE WOULD BE NEEDING A NEW HASH FUNCTION SOON. THE SHA FAMILY (WHICH IS REALLY PART OF THE MD4 AND MD5 FAMILY), WAS UNDER INCREASING PRESSURE FROM NEW TYPES OF CRYPTANALYSIS. WE DIDN'T KNOW HOW LONG THE VARIOUS SHA-2 VARIANTS WOULD REMAIN SECURE. BUT IT'S 2012, AND SHA-512 IS STILL LOOKING GOOD.EVEN WORSE, NONE OF THE SHA-3 CANDIDATES IS SIGNIFICANTLY BETTER. SOME ARE FASTER, BUT NOT ORDERS OF MAGNITUDE FASTER. SOME ARE SMALLER IN HARDWARE, BUT NOT ORDERS OF MAGNITUDE SMALLER. WHEN SHA-3 IS ANNOUNCED, I'M GOING TO RECOMMEND THAT, UNLESS THE IMPROVEMENTS ARE CRITICAL TO THEIR APPLICATION, PEOPLE STICK WITH THE TRIED AND TRUE SHA-512.AT LEAST FOR A WHILE. I DON'T THINK NIST IS GOING TO ANNOUNCE "NO AWARD"; I THINK IT'S GOING TO PICK ONE. AND OF THE FIVE REMAINING, I DON'T REALLY HAVE A FAVORITE. OF COURSE I WANT SKEIN TO WIN, BUT THAT'S OUT OF PERSONAL PRIDE, NOT FOR SOME OBJECTIVE REASON. AND WHILE I LIKE SOME MORE THAN OTHERS, I THINK ANY WOULD BE OKAY. WELL, MAYBE THERE'S ONE REASON NIST SHOULD CHOOSE SKEIN. SKEIN ISN'T JUST A HASH FUNCTION, IT'S THE LARGE-BLOCK CIPHER THREEFISH AND A MECHANISM TO TURN IT INTO A HASH FUNCTION. I THINK THE WORLD ACTUALLY NEEDS A LARGE-BLOCK CIPHER, AND IF NIST CHOOSES SKEIN, WE'LL GET ONE.

Part 6

Language : Tanzanian

CHAMACHAMAPINDUZIPAMOJANAVIJANAWAKEKUPITIAUMOJAWAOWAUVCCMKIMEMSHUKIAALIYEKUWAMWENYEKITIWATUMEYAMABADILIKOYAKATIBAJAJIJOSEPHWARIOBAKIKIMTAKAAACHEKUJIDANGANYAKWANISUALALAKATIBAMPYAHALIWEZIKUWAAJENDAYAUCHAGUZIMKUUMWAKANIKWAUPANDEWAUVCCMIMEMTAKAJAJIWARIOBAAACHEMARAMOJAKUTUMIADHAMANAALIYOKUWAAMEPEWAYAKUWAMWENYEKITIWATUMEYAMABADILIKOYAKATIBAKWANIMUDAWAKEUMEISHAMALIZIKAKISHERIAKAULIHIZOZILITOLEWAKWANYAKATITOFAUTINAVIONGOZIWACHAMAHICHOIKIWANISIKUCHACHETANGUJAJIWARIOBAATOEMAONIYAKEKUHUSIANANARASIMUILIYOPENDEKEZWANABUNGEMAALUMLAKATIBAAMBAPOALIKOSOAKUTOKANANAKUACHWAKWABAADHIYAMAONIYAWANANCHIAIDHAAMEENDELEAKUSISITIZAKUWAATAKUWARAISWAWATANZANIABILAKUJALIDINIKABILAAUVYAMAHIVYOMAENDELEOYASERIKALIYAKEHAYATABAGUAAKIZUNGUMZAJANAMJINIHAPAKWENYEMKUTANOWAKAMPENIULIOHUDHURIWANAMAELFUYAWATUAMBAOALIKIRIKUWANIMKUBWAAMBAOHAJAWAHIKUUONAAMEWAHAKIKISHIAKUWAATAIENDESHANCHIKWAUSTAARABUNASIKWAUDIKTETAKAMAAMBAVYOBAADHIYAWATUWAMEKUWAWAKIDAIHATABAADAYAKUCHAGULIWAMIMISITABADILIKANITABAKIKUWAMTOTOWENUYULEYULEJOHNMAGUFULIA