Computer security – assignment 1

Q1: What is the difference between the symmetric and asymmetric   
cryptosystems?

The symmetric key cryptosystem uses the same key to encrypt as to decrypt.

But the asymmetric key cryptosystem uses a public key to encrypt and

a private key to decrypt.

Q2: What are the main components of any cryptosystem and explain   
them?

There are encryption algorithm, decryption algorithm in any cryptosystem.

Encryption algorithm makes plaintext ciphertext, and decryption algorithm makes ciphertext plaintext. In the encryption and decryption process, a key (or two key) is used.

Q3: Find the plain text of the following Ciphertext generated by Least-  
Simple Substitution (wheel cipher) without knowing the map between  
ciphertext letters and plaintext letters

E GSQTYXIV MW E QEGLMRI XLEX GER FI MRWXVYGXIH XS GEVVC SYX WIUYIRGIW SJ EVMXLQIXMG SV PSKMGEP STIVEXMSRW EYXSQEXMGEPPC ZME GSQTYXIV TVSKVEQQMRK QSHIVR GSQTYXIVW LEZI XLI EFMPMXC XS JSPPSA KIRIVEPMDIH WIXW SJ STIVEXMSRW GEPPIH TVSKVEQW XLIWI TVSKVEQW IREFPI GSQTYXIVW XS TIVJSVQ ER IBXVIQIPC AMHI VERKI SJ XEWOW E GSQTPIXI GSQTYXIV MRGPYHMRK XLI LEVHAEVI XLI STIVEXMRK WCWXIQ QEMR WSJXAEVI ERH TIVMTLIVEP IUYMTQIRX VIUYMVIH ERH YWIH JSV JYPP STIVEXMSR GER FI VIJIVVIH XS EW E GSQTYXIV WCWXIQ XLMW XIVQ QEC EW AIPP FI YWIH JSV E KVSYT SJ GSQTYXIVW XLEX EVI GSRRIGXIH ERH ASVO XSKIXLIV MR TEVXMGYPEV E GSQTYXIV RIXASVO SV GSQTYXIV GPYWXIV GSQTYXIVW EVI YWIH EW GSRXVSP WCWXIQW JSV E AMHI ZEVMIXC SJ MRHYWXVMEP ERH GSRWYQIV HIZMGIW XLMW MRGPYHIW WMQTPI WTIGMEP TYVTSWI HIZMGIW PMOI QMGVSAEZI SZIRW ERH VIQSXI GSRXVSPW JEGXSVC HIZMGIW WYGL EW MRHYWXVMEP VSFSXW ERH GSQTYXIV-EMHIH HIWMKR ERH EPWS KIRIVEP TYVTSWI HIZMGIW PMOI TIVWSREP GSQTYXIVW ERH QSFMPI HIZMGIW WYGL EW WQEVXTLSRIW XLI MRXIVRIX MW VYR SR GSQTYXIVW ERH MX GSRRIGXW LYRHVIHW SJ QMPPMSRW SJ SXLIV GSQTYXIVW ERH XLIMV YWIVW

I guess that first character E is A in plaintext. So shift the encrypted text 4 times, and get this text.

a computer is a machine that can be instructed to carry out sequences of arithmetic or logical operations automatically via computer programming modern computers have the ability to follow generalized sets of operations called programs these programs enable computers to perform an extremely wide range of tasks a complete computer including the hardware the operating system main software and peripheral equipment required and used for full operation can be referred to as a computer system this term may as well be used for a group of computers that are connected and work together in particular a computer network or computer cluster computers are used as control systems for a wide variety of industrial and consumer devices this includes simple special purpose devices like microwave ovens and remote controls factory devices such as industrial robots and computer-aided design and also general purpose devices like personal computers and mobile devices such as smartphones the internet is run on computers and it connects hundreds of millions of other computers and their users

Q4: Decrypt and find the plaintext of the following ciphertext of a message encrypted using Vigenère cipher (Hint: the key is 5 letters)

YBR PMRJHGCW CF N KFWUVLJ NUNR HUA OC NHFGPZWGRB YI PNPWS BHR XYDHCSWRF MK UEVRMGRGGH IE YMLCPNJ TJREYYCBAQ FOGBKFNVPYQFL IGF WBZNZNRE NWITEYRGVAE RIQRPS WBZNZNREQ MUIR RMY NOGQCGL RT ZBYJTQ TRLJLNYGEYQ FCYM BS MUYENRNIAF AFFYRB ULBTPFGF GFJMR CPTAENKX YANZQY PBKUOGRPX NB CCWZBEK FH RKRWYZRJD QVQC WUATC TZ GNQPM N PMRJYRRJ WBZNZNRE GSWYHBNHT GFJ BNEBBUER RMY BCCWUGVLL MLFRJG PBKUOGRP ULBTPFGZVLL CF GFJ JEBAJMF BD IYFVESCAT YSX OHGQXVAE FH RKCHOGNZQY PBKUOGRP ULBTPFG GB YHWBZNQCFU Y XJRPGKCP PMRJHGGSA ERQZFG CPTAENKRCAT GSPBYTJM GNQPM FHAM UF: NLFFLFGX ARACWUGVLL UYTMWCGUKX JEBDNFVAE FFTBPNNUZQ FWPHPFWL NLI LRFMZLPR ATHFHKUNVBL FHQ GFJ CZCJJGRARFNVBL TZ NYETLVGFRM VA Y HBBFCS JEBEWUZZGSA YNLLONTC HIZZMSFL ECKYEECI NB NQ HIQVLL NUR QTOEPC HIQR MK U CEMLLNZ GX QEVRYYA VL THR BP RIER JFHTHYLYF GFFN NEC NHGRJQCTVZQY GB NWITEYRGREQ WUGUCW NUNL RUPUGSY PBBJ QUVAM CF QGWYPGJD YKRAZNRQ ZD NUR AJHGEYQ JEBAJMFVLL OAVR YBR CSWJBFC TZ CEMLLNZKNHT VQ YI SVLI U FROZYAPC TZ VAQYLHPRNIAF RMUG JGQF NHRTGNGC YBR CCWZBEKFHPR MK U GNQP QUVAM WNA ZJ UF PMRJYRV FM NA MUYENRNHT FWXNRZ MS U PBKUOGRP TZGRL KIE FMQPVAE F AVICS JEBZQYZ CPTZVPGJHG CPTAENKRCAT RMOF BDYYA ECVOVECX YKCCWNVFC NH FRTJLNY BNZSRPJHG FSGDRPRX CAPJZXVAE PHBJJJXTR MK NUR YUJYVAFNVBL IIZNGS MCRANUYVXJX NYETLVGFRM NAB KIEZYQ FBTGH NNFIX UPPMRJNAWNHT NLI LRYYYYQ GM ULBTPFGZVLL CAPJZXR GCXNVAE IYOHELCAT QTOEPC HIQR KFCAGCSUAPC NGCYCRYAGYYCBA MK VHVJI MLFRJGF NLI GNAYLYZRLY IS QCWCIRB FLGVDFWGF QZWU NQ YBR ZYHBVAC HIQR MK WBZNZNRE NWITEYRM

I guess first word “YBR” is “The” in plaintext, and if so, the key’s first 3 characters are ‘fun’. Because the key is 5 letters, I decrypt the encrypted message by “funny”, and it seems right.

Key: funny

THE COMPUTER IS A MACHINE THAT CAN BE INSTRUCTED TO CARRY OUT SEQUENCES OF ARITHMETIC OR LOGICAL OPERATIONS AUTOMATICALLY VIA COMPUTER PROGRAMMING MODERN COMPUTERS HAVE THE ABILITY TO FOLLOW GENERALIZED SETS OF OPERATIONS CALLED PROGRAMS THESE PROGRAMS ENABLE COMPUTERS TO PERFORM AN EXTREMELY WIDE RANGE OF TASKS A COMPLETE COMPUTER INCLUDING THE HARDWARE THE OPERATING SYSTEM COMPUTER PROGRAMMING IS THE PROCESS OF DESIGNING AND BUILDING AN EXECUTABLE COMPUTER PROGRAM TO ACCOMPLISH A SPECIFIC COMPUTING RESULT PROGRAMMING INVOLVES TASKS SUCH AS: ANALYSIS GENERATING ALGORITHMS PROFILING ALGORITHMS ACCURACY AND RESOURCE CONSUMPTION AND THE IMPLEMENTATION OF ALGORITHMS IN A CHOSEN PROGRAMMING LANGUAGE COMMONLY REFERRED TO AS CODING THE SOURCE CODE OF A PROGRAM IS WRITTEN IN ONE OR MORE LANGUAGES THAT ARE INTELLIGIBLE TO PROGRAMMERS RATHER THAN MACHINE CODE WHICH IS DIRECTLY EXECUTED BY THE CENTRAL PROCESSING UNIT THE PURPOSE OF PROGRAMMING IS TO FIND A SEQUENCE OF INSTRUCTIONS THAT WILL AUTOMATE THE PERFORMANCE OF A TASK WHICH CAN BE AS COMPLEX AS AN OPERATING SYSTEM ON A COMPUTER OFTEN FOR SOLVING A GIVEN PROBLEM PROFICIENT PROGRAMMING THUS OFTEN REQUIRES EXPERTISE IN SEVERAL DIFFERENT SUBJECTS INCLUDING KNOWLEDGE OF THE APPLICATION DOMAIN SPECIALIZED ALGORITHMS AND FORMAL LOGIC TASKS ACCOMPANYING AND RELATED TO PROGRAMMING INCLUDE TESTING DEBUGGING SOURCE CODE MAINTENANCE IMPLEMENTATION OF BUILD SYSTEMS AND MANAGEMENT OF DERIVED ARTIFACTS SUCH AS THE MACHINE CODE OF COMPUTER PROGRAMS

Q5: What do the following concepts mean:

- Confidentiality is to prevent unauthorized reading of information

- Integrity is to detect unauthorized writing of information

- Availability is that data or service is available in a timely manner when needed

- Hash function makes plaintext ciphertext, but it is one-way, so it cannot make ciphertext plaintext.

- Cryptoanalysis is to check if encryption algorithm is secure or good.

Q6: (optional) Write a simple program in (C, C++, Java, or Python) programming language for Caesar Cipher encryption and decryption. The program accepts the plaintext and shift pattern from user keyboard and print the ciphertext. For decryption, the ciphertext is feed with the shift pattern to the decryption function to get the plaintext. (Include the code in your assignment solution with the output screen from your running program)

#Encyption

def encyption(text, n):

text = text.lower()

res = ""

for i in text:

new = ord(i) + n

if (new > 122):

new -= 26

res += chr(new)

return res

#Decryption

def decryption(text, n):

new = 0

text = text.lower()

res = ""

for i in text:

new = ord(i) - n

if (new < 97):

new += 26

res += chr(new)

return res

#Get plaintext and shift pattern

plainText = input("Enter the plaintext: ")

N = int(input("Enter the shift pattern: "))

#Print the ciphertext

ciphertext = encyption(plainText, N)

print(ciphertext)

#Print the plaintext

plaintext = decryption(ciphertext, N)

print(plaintext)



