Assignment 1

Security and Cryptography (IN4191)

Issue date: 18 Sep 2019
Due date: 30 Sep 2019, 23:59 CET *(hand in via Brightspace)*

- In this assignment you are going to answer questions related to **historical ciphers** and **information theory**.
- This is an individual assignment. Please mention your name and student number in submission. You have to hand in a **SINGLE** document (PDF) with your answers and your source code (if any). **Also, be aware that any form of plagiarism will not be condoned.**
- Pose your questions on the Brightspace forum, so that your fellow students can also read them.
- **Explain and motivate all your answers!**

1. **Classical Systems** *(5 points)*
   In this exercise, you are given several ciphertexts originating from classical systems. For each ciphertext, you need to answer the following questions:

   - Which encryption scheme was used?
   - What was the original plaintext message?
   - What was the encryption key?

   Or explain why it is not possible to decipher it.

   (a) *(1 point)* Consider the ciphertext:
   "JOVJVSHAL DHZ PUCLUALK MVBY AOVBZHUK FLHYZ HNV PU H ZTHSS CPSSHNL PU OVUKBYHZ HUK OHZ AOYPCLK LCLY ZPUJL"

   (b) *(2 points)* Consider the ciphertext:
   "VCALIUTOTNOCINISOMTUPUNLNCADUTSRLUACEAFAO
   CEOXEEWRVTENIESOIAMSNEAMWRCEIHHERTEETCRCOA
   AAETINESEINEHVWNPALIOLETSDHETTEHDFEOOETAAC
   CERNEVEEYTFALULKOIMARSHNEOSDFEAAHRTOTRYWNT
   EOINCLNHIGNAGHNTGHRMFOTERRETESUEKTNIHLIWTF
   IHNEHSTEEATHRTATHORYITYFBUTORSRHWIONMRODLE
   APNESADHSDEENBAEMDEDBDEIEAWNSOTUICVSWSHUPP
   LEIBEHLTHEENTASEMSEVSLTATEIRBTEODERUKTAELH
   AWLIISODHTEITHNWMEHSTEPEMPLTUEABHVYAEEFNHE
   TLIESERTOMNNCETBSYMDUESHCMNUAOADAPCOSSEHMT
   EALNECVSIRNNEAGRAAIEWDCNOEFGORLORFOSYMEAEP
   LOLBOTLWGRRGTIHLETNLEATHOWYEAUDRRPAKCPRERL
   OTIHSNMOCEAKNSIVNALOASARTGEYRELASMYOLRPSUE

CTTHDIEWRCSAERTTOSWRRAOWTIEHLRHERAESECTMLO
POEOYMLSSTWTIHHNIGEADRPEENYITSOIPDFOUSENQU
IATOCCOAASTNHITCTOERHIDLTRNOAEEDTRXUTONSOE
NAERESCSTIEYELDTRHIEMNNEEIERPASSOTSRHTEOTE
FIBNASENXSXDXIE"

(c) *(2 points)* Consider the ciphertext:
"FFX ZSGST UALWLFD CL RTC PVFWR UP FFX ZSGST
UALWLFD CL RTC TUQTSTR IMKSR TG G JUQM VT
CSSYDITIZP QULERKBQEWULE MY JZLGYGOYE HBEWWSURR
NWGST ZK TTYWZIY YGRAVFD WT EGGWLPZCQQ AP IVSXG
VMBSEHF LAULS YGJWPBZ FQJELBTQ ZMGPBZHD. ORRTMNNV
EVK JUQM, PB THY AGPKLBE TUPY, BBK BZH YRMZBSWDS
ALFGE AVP FKLMGLZOYQK, RTC YPFDH YSOF EPGEG UD
ECOLB HCTBQPL KOES LPAK MOS DSIMZB VLBEIXW NA.
MOS ZFOEULTS ZTGZ GZQIPFPR OLZSFLFLPRC HCKZWZBY
RTPHBUS HNC MEXZ, CQHKL XGLAWYU YCHCG LBEFOCE.
MY AVP CXGSGGHZ DSBCZ UHURPFY, MZJR VBP HNC
SPXHH AMXYYGW VT RWFY (MJLV QLZRCP RAL DJFGKUB
HM YSILS, MDMLF EVK NTYKHCS KNM NSBSH TH), ZFQ
MEKSDH UD FFX HBNWKLF UHURPFY PQKTPBD
FKJMRBCSWM OLFYVA. HSS IMXMLZID CL PTMWLG, EVK
JUEAAVZIYC AD TSSIOTBDGT, AVP AGSEMELIX OZ
FMJBJOCBGQESL, AVP HKKBJX VT LFZCYGL HBO HNC
ERTAIP CL XQSL DSCS GJX BXZHCCECP. RAL ZZQGRUMG
HBO IRRUKTAS QOZC AD MOS SOTEULZ NOCRKLE YKL
IYYTMIL, TUR EVKPQ GL ZDPQAJMRBVB EVGR FFXF ALM
TMF FTCS PLOQFCW HH LZR. RTC EPGE QUTQPXK CYZE
RTC LJIWDZSDYE HBO OXATGMLQEIXYX KHUIXSTRE MY AVP
AKBURXYFLBKYZ YGK ATRJJQ CTZHPFT PQEBVBD, KNGOF
MOSY QUKBPBZSO HNC WLHDB HCXJP DHY HSS MPQCDZ.
VPBIC, QVMHBE GORQQ ULMZBJ RTGL YSLZS UQPX UCE
QULEGWLFPR GQ BYKA CQ QULFCFWCCOXW MAVVIYHY. RTC
IYWXOXW MAVVIYHY, AAKBUU QFUK TCESSYWYRUA PYWESXQ,
MJLV VPOBGXW BUTWIKLOCW AVP DRYOCL PBNZABQB BU HSS
CMZBXYG WWYR. RGOL CQ HNC ECOLB PBZPUCL HFP O
ICXCUYOEWUL AD ZYSPY GAOMFWZTGNKQLMZ WY HNC MPMZ
OYR GPOFBASNHAPQ (RAL SIQKNFGHUG MSOLS RAL DJFGKUBL
VT RWFY MLW AVP VGLSGGN ULFJCZQ HM PLPEJAL). MOS
DSBCZ UHURPFY MZ YGAWAOZCD'Q EPGE KUL BPTPGPG LMD
RALWC BURMZEL TPOZSDCL, YOYUOLS DKVA DIVCDJTAWGSY
MR RAL VTUNCER HY ZLFMCER HM HSSOP FWILG, EC ZFQ
YKAWDHXW IGMO KSWIF FFXF KPFK CJCVBHPR. ZFQGK
HFNVORQAMBFLZ GLP YKAWDHOA RCTAICSY UQPX PATHGRQB
MOFZIMFASM AVP VKJXCGPGEWI UAPEK OYR HCKMGK. HSS
MPQCD PBQZACZAX PB CCSYZ ANSHFFK, YZB MOS CSBGHYE
VT RFKAA-PHTOY OXRUQMPQ DHEJQQ WBFTBM RTC
KLBLWYQMLVL QLIMFF RAL WXOMGZYMPCY CL CGPHWSLB

GPFGLAG LBJ RDYOLZWSXQ. BYBUHTBMQ MLW ZQFZVRGPXZ
OWZABULZ AC LBZGBYMLF'D ZOQF UXYS XOJC, IFBSS
LRBCZRNYSCG LJAADLR EC ZFQ YVAILZ YGFCL AC
ASXQALTSZJ KORZCLZ HSS CMZBXYG. WSMCZBL
JWCQAJMRXK HZ TAPFFXY QZAVJQKXUH EVK
QGNXYZLHOTQQ HM HSS CMZBXYG."

2. **Security Games** *(2 points)*
   Draw the security game for a family of pseudo-random permutations $\{F_k\}_K$, for an attacker A with access to two oracles: $\mathcal{O}_{F_k}$ and $\mathcal{O}_{F_k}^{-1}$.

3. **Information Theoretic Security** *(3 points)*
   We have the following sets of possible plaintexts, keys and ciphertexts:

$$\mathbb{P} = \{a, b, c, d\}$$

$$\mathbb{K} = \{k_1, k_2, k_3, k_4\}$$

$$\mathbb{C} = \{1, 2, 3, 4\}$$

   The plaintexts and keys have the following probabilities:

$$p(\cdot) = \left\{a = \frac{2}{7}, b = \frac{1}{7}, c = \frac{3}{7}, d = \frac{1}{7}\right\}$$

$$p(\cdot) = \left\{k_1 = \frac{1}{4}, k_2 = \frac{1}{4}, k_3 = \frac{1}{4}, k_4 = \frac{1}{4}\right\}$$

   Consider the encryption scheme listed in Table 1.

	a	b	c	d
k_1	4	1	3	2
k_2	1	3	2	4
k_3	2	4	1	3
k_4	4	2	1	3

Table 1: Encryption scheme

   (a) *(1 point)* Calculate the probability of each plaintext conditioned on each ciphertext occurrence.

   (b) *(½ point)* Compute the entropy $H(P|C = 4)$.

   (c) *(½ point)* Compute the entropy $H(P|C)$.

   (d) *(1 point)* Is this scheme perfectly secure?

Before you submit your solutions:

- Make sure all your answers are **properly explained** and include your **calculations**!