**COMP7906A Introduction to Cyber Security**

**Assignment 1**

**(Due on 29 Sep 2024, 23:59)**

Q1. Referring to the lecture notes on DES, there are one Expansion Permutation (Table1), eight Substitution S-Boxes and one Permutation P-Box (Table 2) in the function f(Ki, Ri) for round i in DES encryption. Given that the input plain text is A7E2BC3FD4C896D2 and the encryption key is1A5D6D895B4B66DB in hexadecimal representation. Implement round 1 encryption manually and list L1 and R1. The initial permutation for input is shown in table 3.

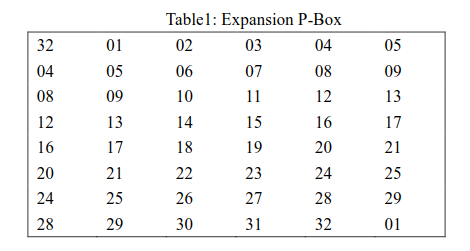
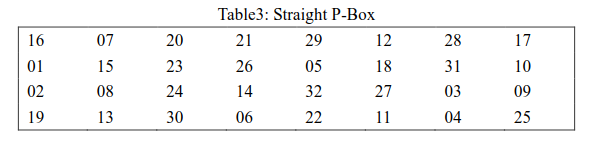
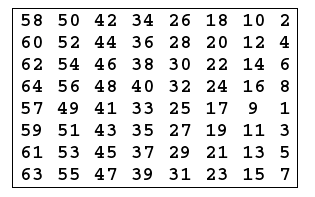
Table 1: Expansion Permutation

Table 2: Permutation P-Box

Table 3: Input Permutation

**We recommend you show your intermediate results in order to earn partial credits.**

Q2. An English prose quotation is encrypted with an unknown method. Below is the encrypted quotation (where spaces between words are suppressed).

fjwvs yfvbl hfwdu skevm wiodm bmiff wmhhu vzsxj iqjvs zfvhv

bvvjp hepqe dfrjs swtif zolmp hzzhz xiyxe wliem wrhww ubufi

ylubh rbryt jdths revbr rwwjl hkcvi wyofd jimuw zcfwi csjka

xiuvz osren kvdsg jzltd svucf lzsvm swyfg yhbdj ssrbh gkvwt

bwlww umtfd erkjp lxdhz vfybv ojwba rrikx suozo kidou vrsrj

hdlum vbfvv oleun kvssw uuvzo kyngl ktgpm izzby mumdt qwwtc

rehgx iywis sxzii raaxz uquqg sqyur hasou xjhje mcdzg sqfge

vfgju bhtce qphzv odxii ieolm phvzb oljwk kvwgp gpfbo ibfwy

vweem rwugz flqds fxnyh kwfkt jufja hfnkv asmoz riiej plffc

hisuw zcfev mwiod mbbdj sfisa hkwue mfbgi jwvyg kvwgb ovvcx

monhi bsxji qrzlv bxhcw tisuo zgsxj iqrik xsuoz odien kvtgv

nuwzc fsgnk vqsms hvxfg yququ okmbj dtwxm dyffb gqjwf fchis

uwzcf mucvr awqcy uftll fiuxo fmtuw zcfjp lhtcf sncft cgtfl

dkwgr bhgus nimis dsfxb hgkvw aplou hjeey riusr jtdkw grubh

issvf mhmsj emgda cjfjf dksje mzuvs lvbxh rujif ghehk evmwi

odmbb djdmv tohua gwulh tsfxm swyss ytnur zaevh lksvw uuwvg

xvfyw iovib auvse ionde ruppm hisus oipzq jimuw zcfwx cwybw

aaydc ofhbz rlbvm oapva tiswr lblvz iikvw yocwv rfeuc regsy

tnurz aebfv fasmo ndzbk eocqk sjrbn lfbsp bcggf gksup lbvis

qkzqz wpghj wpxzw rlblv jyvis uijph rgkmt ndeqw xiyel ryiuj

ufjah fmrms jxxid erslb fiswd pjiqw cjhfp hcchq fhwrg kmtnd

eqwet usvfu iondx sgjhx skvaw diqkf afvnl fbawm yvjhz eonkr

hgjub hlbem mfheb aynxh msdsq ghehy sbfv

Analyze the encryption to answer the following questions:

(a) What type of cipher is it? (Monoalphabetic / Polyalphabetic) Briefly explain.

(b) Give the permutation(s) (if any) or the substitution(s) used in the cipher. Briefly explain.

(c) Recover the cipher text into plain text.

Q3. Break the following ciphertext.

qeFIP?eGSeECNNS

5coOMXXcoPSZIWoQI

avnl1olyD4lylDohww6DhzDjhuDil

z.GM?.cEQc. 70c.7KcKMKHA9AGFK

?MFYp2pPJJUpZSIJWpRdpMFY

ZqH8sl5HtqHTH4s3lyvH5zH5spH4t pHzqHlH3l5K

Zfbi!tif!xpvme!qspcbcmz!fbu!nfA

Q4. Password Guessing

Assume you want to maintain low security (Level 1) with password guessing probability 1 in 210 .

Assume n = 10, b = 95 printable characters, G = 100 billion guesses per second (assume using GPU).

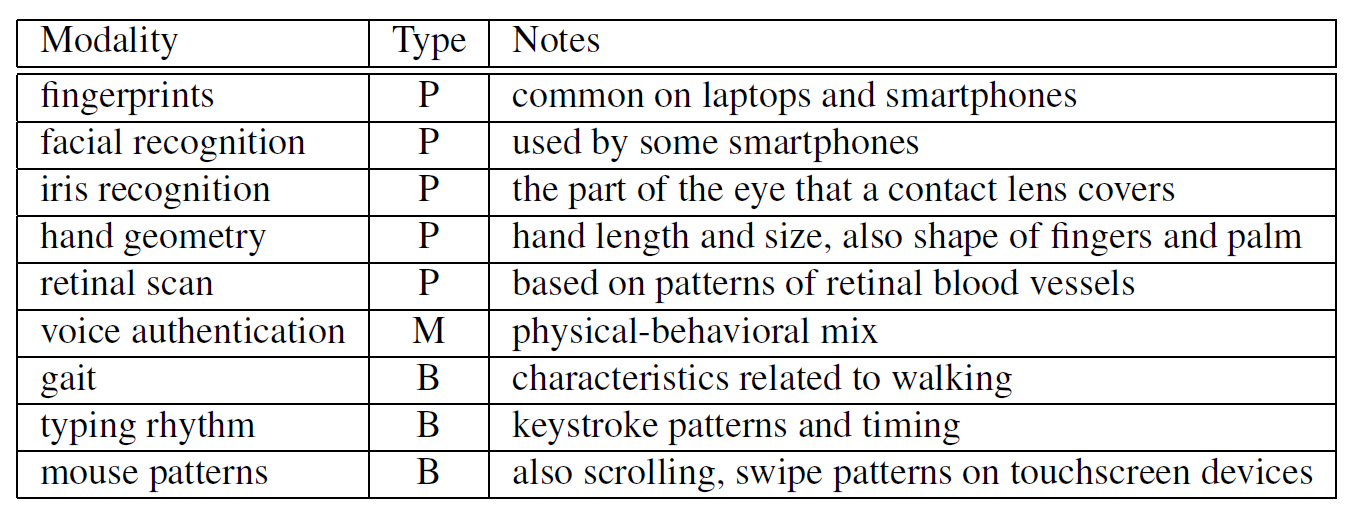
What should be the password expiration policy?

Q5. NIST SP 800-63B

U.S. government password guidelines were substantially revised in 2017

1. What are the key features w.r.t. to our discussion in class?
2. Any similar guidelines in China? Compare the guidelines in China with the NIST SP 800-63B.

Q6. Circumventing Biometrics



Select one biometric modality in the above table. Identify possible modality-specific attacks for the selected modality.