COMP5631: Cryptography and Security
2025 Spring – Written Assignment Number 2
Handed out: on Feb. 21, 2023
Due: on March 9 by 11:30pm.

Please upload your solution paper into Canvas by 23:30 on March 9. No email submission will be accepted.

Q1. Please read the transposition cipher documented in the Appendix of Lecture 2. Then use the example transposition cipher on Slide No. 25 to encrypt the message `killthem`. Write down the corresponding ciphertext. $\boxed{\text{10 marks}}$

Solution: Let us apply the transposition cipher with the following permutation function:

$$\begin{aligned} f : i &\mapsto f(i) \\ 0 &\mapsto 2 \\ 1 &\mapsto 0 \\ 2 &\mapsto 3 \\ 3 &\mapsto 1 \end{aligned}$$

Arranging the plaintext `killthem` in blocks of 4:

$$\begin{matrix} \text{k} & \text{i} & \text{l} & \text{l} \\ \text{t} & \text{h} & \text{e} & \text{m} \end{matrix}$$

Applying the permutation f to each block yields the ciphertext:

`lkli etmh`

Q2. There are ten pieces of ciphertext in the following URL:
[Click here]
Each of them is obtained by encrypting an English article with a simple substitution cipher. Let ℓ denote the last digit in your student ID number, please then choose the $((\ell + 1) \bmod 10)$-th ciphertext and recover the original plaintext.

You may write your own computer programs or use the following online software to compute the frequencies of single letters, digraphs and trigraphs in the ciphertext for you:

```
https://www.cryptoclub.org/#vCiphers
```

Please write down certain details of your decryption process. You need to write down your decrypted text (i.e., the readable text), but do not need to write down the one-to-one function used for encryption. $\boxed{\text{30 marks}}$

Solution: The last digit of my student ID is 2, so I will decrypt the 3rd ciphertext. The ciphertext is as follows:

```
YBWCYXMVZYQGVRHAWKDX YQVGDXLVGLQWRQDICDR HKWRWIQDIYIPIBDFWBM
HBYXW: HWVHBW'R QWWQA. YXXVKUDICQV YKWHVKQHPLBDRAWU QVUYMDIQAW
EVPKIYBIYQPKW, LVGL-CWIWKYQWU XYKLVIDRVQVHWR QKYHHWUDI QVVQAWIYGWB
GYMHKVTDUWYGVKW HKWXDRWGWQAVU ZVKUWQWKGDIDICYUWXWYRWU DIUDTDUPYB'R
YCWQAYIVQAWKZVKWIRDX GWQAVURXYI.

QAWYLVTWCKVPIU IPXBWYKQWRQRQAYQVXXPKKWU LWQNWWI 1955 YIU 1963
UKYGYQDXYBBM DIXKWYRWUQAW YGVPIQVZQAW DRVQVHWXYKLVI 14 DIQAW
YQGVRHAWKW. QAWBWTWBRKYHDUBM WOPYBDSWUYKVPIUQAW CBVLW, WTWI
QAVPCAQAWWJHBVRDVIR VXXPKKWU YQVIBMYZWN BVXYQDVIR, YIUWIQWKWU
HBYIQRDIQAWZVVU XAYDIQAKVPCA HAVQVRMIQAWRDR. LM WYQDICHBYIQR,
YIUYIDGYBR QAYQZWWUVIHBYIQR, APGYIRYLRVKL XYKLVI 14 YIUWJADLDQ
BWTWBRVZ QAWLWIDCI, QKYXWYLBW DRVQVHWQAYQ YKWRDGDBYK QVYQGVRHAWKDX
XVIXWIQKYQDVIR. NAYQDRGVKW, XYKLVI 14 UWXYMRNDQAY AYBZ-BDZWVZ
5,730 MWYKR, YHAWIVGWIVI QAYQRXDWIQDRQR XYIWJHBVDQ YRYNYMQV
UWQWKGDIW QAWYCWRVZVLEWXQR QAYQXVIQYDI QAWDRVQVHW. ZVKQAWIWN
RQPUM, EVIYRZKDRWI VZQAWGWUDXYB IVLWBDIRQDQPQW DIRQVXFAVBG,
RNWUWI, YIUADRXVBBWYCPWR YIYBMSWUQAWXYKLVI XVIQWIQVZQVVQAWIYGWB.
LWXYPRWQWWQA UVIVQWJADLDQYIM QPKIVTWKUPKDIC YHWKRVI'R BDZW,
QAWRXDWIQDRQR XYIUWQWKGDIW NAWIYQVVQAZVKGWU LMXVGHYKDICDQR
XYKLVI 14 XVIQWIQQVHYRQ YQGVRHAWKDXBWTWBR. DIYUUDQDVI, YUPBQ
QWWQAZVKGUPKDICY UDRQDIXQHWKDVU VZXADBUAVVU UWTWBVHGWIQYKVPIU
YCW 12, RVQADRDIZVKGYQDVI XYILWQKYIRBYQWUDIQV QAWYCWVZYI
DIUDTDUPYB.
```

1. I wrote the decryption code myself, and the code is attached in the supplementary files. The code is written in Python. Below are the steps I followed to decrypt the ciphertext.
2. I first replaced all alphabets according to the frequency of English letters. The resulting text is:

```
aceralyogatmoiuheswl atomwlbombteitwnrwi useientwnanpncwjecy
ucale: ueouce'i teeth. allosdwnrto aseuostupbcwihed todaywnthe
xopsnacnatpse, bomb-renesated lasbonwiotouei tsauuedwn toothenamec
mayusofwdeamose uselwiemethod gosdetesmwnwnradeleaied wndwfwdpac'i
arethanothesgoseniwl methodilan.

theabofersopnd nplceasteitithatollpssed between 1955 and 1963
dsamatwlaccy wnlseaiedthe amopntogthe wiotouelasbon 14 wnthe
atmoiuhese. thecefecisauwdcy ezpacwqedasopndthe rcobe, efen
thoprhtheekucoiwoni ollpssed atoncyagev colatwoni, andentesed
ucantiwnthegood lhawnthsoprh uhotoiyntheiwi. by eatwnrucanti,
andanwmaci thatgeedonucanti, hpmaniabiosb lasbon 14 andekhwbwt
cefeciog thebenwrn, tsaleabce wiotouethat aseiwmwcas toatmoiuheswl
lonlentsatwoni. vhatwimose, lasbon 14 delayivwtha hacg-cwgeog
5,730 yeasi, auhenomenon thatilwentwiti lanekucowt aiavayto
detesmwne theareiogobxelti thatlontawn thewiotoue. gosthenev
itpdy, xonaigswien ogthemedwlac nobecwnitwtpte wnitoljhocm,
```

```
iveden, andhwiloccearpei anacyqedthelasbon lontentogtoothenamec.
belapieteeth donotekhwbwtany tpsnofesdpswnr auesion'i cwge,
theilwentwiti landetesmwne vhenatoothgosmed bylomuaswnrwti
lasbon 14 lontenttouait atmoiuheswlcefeci. wnaddwtwon, adpct
teethgosmdpswnra dwitwnltueswod oglhwcdhood defecoumentasopnd
are 12, iothwiwngosmatwon lanbetsanicatedwnto theareogan
wndwfwdpac.
```

3. I then manually replaced some words to improve readability:

```
acesalyogatmoiuhervl atomvlbombteitvnsvi ureientvnanpncvjecy
ucale: ueouce'i teeth. allordvnsto areuortupbcvihed todayvnthe
xoprnacnatpre, bomb-senerated larbonviotouei trauuedvn toothenamec
mayurofvdeamore urelviemethod gordetermvnvnsadeleaied vndvfvdpac'i
asethanothergorenivl methodilan.

theabofesropnd nplcearteitithatollprred between 1955 and 1963
dramatvlaccy vnlreaiedthe amopntogthe viotouelarbon 14 vnthe
atmoiuhere. thecefecirauvdcy ezpacvqedaropndthe scobe, efen
thopshtheekucoivoni ollprred atoncyagew colatvoni, andentered
ucantivnthegood lhavnthropsh uhotoiyntheivi. by eatvnsucanti,
andanvmaci thatgeedonucanti, hpmaniabiorb larbon 14 andekhvbvt
cefeciog thebenvsn, traleabce viotouethat areivmvcar toatmoiuhervl
lonlentratvoni. whatvimore, larbon 14 delayiwvtha hacg-cvgeog
5,730 yeari, auhenomenon thatilventviti lanekucovt aiawayto
determvne theaseiogobxelti thatlontavn theviotoue. gorthenew
itpdy, xonaigrvien ogthemedvlac nobecvnitvtpte vnitoljhocm,
iweden, andhvilocceaspei anacyqedthelarbon lontentogtoothenamec.
belapieteeth donotekhvbvtany tprnoferdprvns auerion'i cvge,
theilventviti landetermvne whenatoothgormed bylomuarvnsvti
larbon 14 lontenttouait atmoiuhervlcefeci. vnaddvtvon, adpct
teethgormdprvnsa dvitvnltuervod oglhvcdhood defecoumentaropnd
ase 12, iothvivngormatvon lanbetranicatedvnto theaseogan
vndvfvdpac.
```

4. After further refinement, the final decrypted plaintext is:

```
alegacyofatmospheric atomicbombtestingis presentinanunlikely
place: people's teeth. accordingto areportpublished todayinthe
journalnature, bomb-generated carbonisotopes trappedin toothenamel
mayprovideamore precisemethod fordeterminingadeceased individual's
agethanotherforensic methodscan.

theaboveground nucleartteststhatoccurred between 1955 and 1963
dramatically increasedthe amountofthe isotopecarbon 14 inthe
atmosphere. thelevelsrapidly equalizedaroundthe globe, even
thoughtheexplosions occurred atonlyafew locations, andentered
plantsinthefood chainthrough photosynthesis. by eatingplants,
andanimals thatfeedonplants, humansabsorb carbon 14 andexhibit
```

```
levelsof thebenign, traceable isotopethat aresimilar toatmospheric
concentrations. whatismore, carbon 14 decayswitha half-lifeof
5,730 years, aphenomenon thatscientists canexploit asawayto
determine theagesofobjects thatcontain theisotope. forthenew
study, jonasfrisen ofthemedical nobelinstitute instockholm,
sweden, andhiscolleagues analyzedthecarbon contentoftoothenamel.
becauseteeth donotexhibitany turnoverduring aperson's life,
thescientists candetermine whenatoothformed bycomparingits
carbon 14 contenttopast atmosphericlevels. inaddition, adult
teethformduringa distinctperiod ofchildhood developmentaround
age 12, sothisinformation canbetranslatedinto theageofan
individual.
```

The mapping relationship between the original ciphertext and the decrypted plaintext is as follows:

```
{'A': 'h', 'B': 'l', 'C': 'g', 'D': 'i', 'E': 'j', 'F': 'x', 'G': 'm', 'H': 'p',
'I': 'n', 'J': 'k', 'K': 'r', 'L': 'b', 'M': 'y', 'N': 'w', 'O': 'z', 'P': 'u',
'Q': 't', 'R': 's', 'S': 'q', 'T': 'v', 'U': 'd', 'V': 'o', 'W': 'e', 'X': 'c',
'Y': 'a', 'Z': 'f'}
```

Q3. Consider the example cipher on Slide No. 22 of Lecture 3, where p is a prime. Let $\ell = 2$ (i.e., the cipher has two rounds of iteration of the round function $f_h(x)$). Write down the encryption function $E_k(m)$ and decryption function $D_k(c)$ of this cipher. $\boxed{\text{20 marks}}$

Solution:

For the two-round cipher where $\ell = 2$, we have:

1) The round function $f_h(x)$ is:

$$f_h(x) = ((x + h)^3 + h) \bmod p$$

2) **Encryption Function** $E_k(m)$:

$$\begin{aligned} E_k(m) &= f_{k_2}(f_{k_1}(m)) \\ &= \left(\left(((m + k_1)^3 + k_1) + k_2\right)^3 + k_2\right) \bmod p \end{aligned}$$

3) **Decryption Function** $D_k(c)$:

The inverse round function is:

$$f_h^{-1}(x) = ((x - h)^u - h) \bmod p$$

where u is the multiplicative inverse of 3 modulo $(p - 1)$

Therefore:

$$\begin{aligned} D_k(c) &= f_{k_1}^{-1}(f_{k_2}^{-1}(c)) \\ &= ((((c - k_2)^u - k_2) - k_1)^u - k_1) \bmod p \end{aligned}$$

where: - $k_1 = \alpha^{k+1} \bmod p$ - $k_2 = \alpha^{k+2} \bmod p$

Q4. Given a one-key block cipher $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k)$, where $\mathcal{M} = \mathcal{C}$ and E_k maps an n-bit block into an n-bit block, we can construct a new one-key block cipher by picking up two keys k_1 and k_2 for the original cipher to form a key $k = (k_1, k_2)$ for the new block cipher. The encryption and description of the new cipher go as follows:

Encryption: $c = E_{k_2}(E_{k_1}(m))$.
Decryption: $m = D_{k_1}(D_{k_2}(c))$.

Thus the new block cipher has the same block length as the original cipher, but its key length doubles that of the original cipher. This is the double encryption introduced in Lecture 5.

Design a specific one-key cipher and show that double-encryption with this cipher does not increase the security level of the original cipher at all. [Hint: Consider some of the ciphers on some lecture sides.] $\boxed{\text{20 marks}}$

Solution:

We design a specific one-key block cipher where double encryption does not increase security. Let the message space $\mathcal{M}$, ciphertext space $\mathcal{C}$, and key space $\mathcal{K}$ be $\{0,1\}^n$. Define the encryption and decryption operations as follows:

- **Encryption:** $E_k(m) = m \oplus k$
- **Decryption:** $D_k(c) = c \oplus k$

For double encryption with keys k_1 and k_2, the process becomes:

$$E_{k_2}(E_{k_1}(m)) = E_{k_2}(m \oplus k_1) = (m \oplus k_1) \oplus k_2 = m \oplus (k_1 \oplus k_2).$$

This is equivalent to a single encryption with the key $k_3 = k_1 \oplus k_2$. Therefore, the effective key space remains $\{0,1\}^n$, not $\{0,1\}^{2n}$. An attacker can brute-force the key in $O(2^n)$ time, identical to the original cipher. Thus, double encryption provides no security improvement.

Q5. Show that the Diffie-Hellman Key Exchange (Agreement) Protocol is insecure with respect to active attacks. $\boxed{\text{20 marks}}$

Solution:

The Diffie-Hellman Key Exchange (DHKE) protocol is vulnerable to man-in-the-middle (MITM) attacks. Here's a demonstration:

1. **Normal Protocol Operation** - Public parameters: prime p, generator g - Alice chooses secret a, sends $A = g^a \bmod p$ to Bob - Bob chooses secret b, sends $B = g^b \bmod p$ to Alice - Shared key: $K = g^{ab} \bmod p$

2. **MITM Attack Process** - Eve intercepts all communications - When Alice sends A: * Eve intercepts A * Eve chooses e, sends $E = g^e \bmod p$ to Bob - When Bob sends B: * Eve intercepts B * Eve sends $E = g^e \bmod p$ to Alice

3. **Result** - Alice computes key $K_1 = g^{ae} \bmod p$ - Bob computes key $K_2 = g^{be} \bmod p$ - Eve knows both K_1 and K_2 - Eve can decrypt all messages - Alice and Bob have different keys but don't know it

This shows DHKE is insecure against active attacks without proper authentication mechanisms.