# Лабораторна робота 3 з Симетричної Криптографії

## Варіант - 1

Студентів ФІ-03 Дигаса Богдана та Антоненко Макара

### Покладемо початкові значення

In [ ]:
```
from collections import Counter

alphabet = "абвгдежзийклмнопрстуфхцчшщьыэюя"
m = len(alphabet)

f = open("encrypted_text.txt", "r", encoding = 'utf-8')
encrypted_text = f.read()
f.close()
```

### Проведемо препроцесинг

In [ ]:
```
def check_preprocessing(text):
    for char in text:
        if char not in alphabet:
                print("Faulty letter is:", char)
                return False
    return True

print(check_preprocessing(encrypted_text))
```

```
Faulty letter is:

False
```

In [ ]:
```
def preprocess_text(text):
    formatted_text = ""
    for char in text:
        if 'а' <= char and char <= 'я':
            formatted_text += char
        elif 'А' <= char <= 'Я':
            formatted_text += char.lower()
        elif char == 'Ё' or char == 'ё':
            formatted_text += 'е' # not pasting everything that is not al
    return formatted_text

encrypted_text = preprocess_text(encrypted_text)
print(check_preprocessing(encrypted_text))
```

```
True
```

### Напишемо допоміжні функції, що знадобляться нам у цьому нелегкому ділі

In [ ]:
```python
def extended_euclidean_algorithm(a, b):
    if b == 0:
        return a, 1, 0

    gcd, v_prev, u_prev = extended_euclidean_algorithm(b, a % b)
    u = u_prev
    v = v_prev - (a // b) * u_prev

    return gcd, u, v

def multiplicative_inverse(a, m):
    gcd, x, _ = extended_euclidean_algorithm(a, m)
    if gcd == 1:
        return x % m
    else:
        return "The multiplicative inverse does not exist."

def solve_linear_congruence(a, b, n):
    d, a_coef, _ = extended_euclidean_algorithm(a, n)
    if d == 1:          # тоді a^-1 = a_coef
        return [(a_coef * b) % n]
    elif b % d == 0:
        a_1, b_1, n_1 = a // d, b // d, n // d
        _, a_1_inv, _ = extended_euclidean_algorithm(a_1, n_1)
        x_0 = (a_1_inv * b_1) % n_1
        return [x_0 + k * n_1 for k in range(d)]
    else:
        return []
```

## Визначимо 5 біграм, які зустрічаються у нашому тексті найчастіше:

In [ ]:
```python
# Обчислення частоти біграм
bigram_frequency = Counter([encrypted_text[i:i+2] for i in range(0, len(e

# Знаходження найчастіших біграм
most_common_bigrams_encrypted = []
for i in range(5):
    most_common_bigrams_encrypted.append(bigram_frequency.most_common(5)[
print("Найчастіші біграми у моєму зашифрованому тексті:", most_common_big

most_common_bigrams_open = ['ст','но', 'то','на','ен'] # з умови
print("Найчастіші біграми у звичайному, відкритому тексті:", most_common_
```

```
Найчастіші біграми у моєму зашифрованому тексті: ['рн', 'ыч', 'нк', 'цз',
'иа']
Найчастіші біграми у звичайному, відкритому тексті: ['ст', 'но', 'то', 'н
а', 'ен']
```

## Напишемо код для знаходження ключів шляхом комбінації найбільш ймовірних біграм та розв'язання системи рівнянь для неї:

In [ ]:
```
def bigram_match(bigram):
    return alphabet.index(bigram[0]) * m + alphabet.index(bigram[1])

def get_keys(best_encrypted):
    keys = []
    for i_1 in range(5):
        for j_1 in range(5):
            for i_2 in range(5):
                for j_2 in range(5):
                    if i_1 == i_2 and j_1 == j_2:
                        continue

                    X_1 = bigram_match(most_common_bigrams_open[i_1])
                    Y_1 = bigram_match(best_encrypted[j_1])
                    X_2 = bigram_match(most_common_bigrams_open[i_2])
                    Y_2 = bigram_match(best_encrypted[j_2])

                    A = solve_linear_congruence(X_1 - X_2, Y_1 - Y_2, m**
                    keys += [(a, (Y_1 - a * X_1) % m**2) for a in A]
    return keys

def bigram_unmatch(X_i):
    x_2i_1 = X_i // m       # x_{2i-1}
    x_2i = X_i - x_2i_1*m     # x_{2i}
    return x_2i_1, x_2i

def bigram_decrypt(key, Y_i):
    (a, b) = key
    X_i = (multiplicative_inverse(a, m**2) * (bigram_match(Y_i) - b)) % m
    return bigram_unmatch(X_i)
```

Тепер напишемо функцію яка буде розшифровувати текст для заданого ключа:

In [ ]:
```
def try_decrypt_text(text, key):
    (a, _) = key
    (d, _, _) = extended_euclidean_algorithm(a, m**2)
    if d != 1:
        return "Invalid!"

    res = ""
    for i in range(1, len(text), 2):
        encr = text[i - 1] + text[i]
        x1, x2 = bigram_decrypt(key, encr)
        res += alphabet[x1] + alphabet[x2]
    return res
```

Оскільки ми не впевнені що розшифрований текст буде правильний (впевнені що буде багато неправильних, адже це такий розумний брутфорс, але все ще брутфорс), напишемо функцію для перевірки чи наш текст має сенс за критерієм заборонених l-грам.

In [ ]:
```
def check_if_contains_bigrams(text, bigrams):
    for bigram in bigrams:
        if bigram in text:
            return True
    return False

def check_if_text_makes_sense(text):
    if check_if_contains_bigrams(text, ["аь", "еь", "оь", "уь", "иь", "ыь
        return True
```

Зберемо все що ми написали в одну функцію!

In [ ]:
```
def affine_decrypt(text, bigrams):
    my_keys = get_keys(bigrams)
    for key in my_keys:
        open_text = try_decrypt_text(text, key)
        if open_text == "Invalid!":
            continue
        if check_if_text_makes_sense(open_text):
            continue
        return open_text, key

print(affine_decrypt(encrypted_text, most_common_bigrams_encrypted))
```

('многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписа
телякакневротикакакмыслителяэтикаикакгрешникакакжеразобратьсявэтойневольн
осмущающейнассложностинаименееспоренонкакписательместоеговодномрядусшексп
иромбратьякарамазовывеличайшийроманизвсехкогдалибонаписанныхалегендаовели
коминквизитореодноизвысочайшихдостиженийміровойлитературыпереоценитькотор
оеневозможноксожалениюпередпроблемойписательскоготворчествапсихоанализдол
женсложитьоружиедостоевскийскореевсегоуязвимкакморалистпредставляяегочело
векомвысоконравственнымнатомосновании чтотолькототдостигаетвысшегонравстве
нногосовершенствактопрошелчерезглубочайшиебездныгреховностимыигнорируемод
носоображениеведьнравственнымявляетсячеловекреагирующийуженавнутреннеиспы
тываемоеискушениеприэтомемунеподдаваяськтожепопеременнотогрешиттораскаива
ясьставитсебевысокиенравственныецелитоголегкоупрекнутьвтомчтоонслишкомудо
бнодлясебястроитсвоюжизньоннеисполняетосновногопринципанравственностинеоб
ходимостиотречениявтовремякакнравственныйобразжизнивпрактическихинтересах
всегочеловечестваэтимоннапоминаетварваровэпохипереселениянародовварварову
бивавшихизатемкаявшихсявэтомтакчтопокаяниестановилосьтехническимпримеромр
асчищавшимпутькновымубийствамтакжепоступаливангрозныйэтасделкассовестьюха
рактернаярусскаячертадостаточнобесславиконечныйитогнравственнойборьбыдо
стоевскогопослеисступленнойборьбывоимяпримиренияпритязанийпервичныхпозыво
виндивидастребованиямичеловеческогообществаонвынужденнорегрессируеткподчи
нениюмирскомуидуховномуавторитетукпоклонениюцарюихристианскомубогукрусско
мумелкодушномунационализмукчемуменеезначительныеумыпришлисгораздоменьшими
усилиямичемонвэтомслабоеместобольшойличностидостоевскийупустилвозможность
статьучителемиосводителемчеловечестваиприсоединилсяктюремщикамкультураб
удущегонемногимбудетемуобязанавэтомповсейвероятностипроявилсяегоневрозизз
аторогоонибылосужденнатакуюнеудачупомощипостиженияисилелюбвиклюдямемубы
лоткрытдругойапостольскийпутьслужениянампредставляетсяотталкивающимрассма
триваниедостоевскоговкачествегрешникаилипреступниканоэтоотталкиваниенедол
жноосновыватьсянаобывательскойоценкепреступникавыявитьподлиннуюмотивацию п
реступлениянедолгодляпреступникасущественныдвечертыбезграничноесебялюбиеи
сильнаядеструктивнаясклонностьобщимдляобеихчертипредпосылкойдляихпроявлен
ийявляетсябезлюбовностьнехваткаэмоциональнооценочногоотношениякчеловекуту
тсразувспоминаешьпротивоположноеэтомуудостоевскогоегобольшуюпотребностьвл
юбвиегоогромнуюспособностьлюбитьпроявившуюсявегосверхдоброте ипозволявшую
емулюбитьипомогатьтамгдеонимелбыправоненавидетьимстить напримерпоотношению
кегопервойженеиеелюбовникунотогдавозникаетвопросоткудаприходитсоблазнприч
ислениядостоевскогокпреступникамответиззавыбораегосюжетовэтопреимуществен
ноналсильникиубийцыэгоцентрическиехарактерычтосвидетельствуетосуществовани
итакихсклонностейвеговнутреннеммиреатакжеиззанекоторыхфактовегожизнистрас
тиегоказартнымиграмможетбытьсексуальногорастлениянезрелойдевочкиисповедьэ
топротиворечиеразрешаетсяследующимобразомсильнаядеструктивнаяустремленнос
тьдостоевскогокотораямоглабысделатьегопреступникомбылавегожизнинаправлена
главнымобразомнасамогосебявовнутрьвместотогочтобыизнутриитакимобразомвыра
зилассьвмазохизмеичувствевинывсетакивеголичностинемалоисадистическихчертвы
являющихсявегораздражительностимучительстве нетерпимостидажепоотношениюклю
бимымлюдяматакжевегоманереобращениясчитателемитаквмелочахонсадиствовневва
жномсадистпоотношениюксамомусебеследовательномазохистиэтомягчайшийдоброду
шнейшийвсегдаготовыйпомочьчеловеквсложнойличностидостоевскогомывыделилитр
ифактораодинколичественныйидвакачественныхегочрезвычайноповышеннуюаффекти
вностьегоустремленностькперверзиикотораядолжнабылапривестиегоксадомазохиз
муилисделатьпреступникомиегонеподдающееясяанализутворческоедарованиетакоес
очетаниевполнемоглобысуществоватьибезневрозаведьбываютжестопроцентныемазо
хистыбезналичияневрозовпосоотношениюсилпритязанииипервичныхпозывовипротиво
борствующихимторможенийприсоединяясюдавозможностисублимированиядостоевско
говсеещеможнобылобыотнестикразрядуимпульсивныххарактеровноположениевещейз
атемняетсяналичиемневрозанеобязательногокакбылосказаноприданныхобстоятель
ствахновсежевозникающеготемскореечемнасыщенноеосложнениеподлежащеесосторо
нычеловеческогояпреодолениюневрозэтотолькознактогочтоятакойсинтезнеудался
чтоноприэтойпопыткепоплатилосьсвоимединствомвчемжевстрогомсмыслепроявляе
тсяневроздостоевскийназывалсебясамидругиетакжесчиталиегоэпилептикомнатомо

```
снованиичтоонбылподвержентяжелымприпадкамсопровождавшимисяпотерейсознания
судорогамиипоследующимупадочнымнастроениемвесьмавероятночтоэтатакназываем
аяэпилепсиябылалишьсимптомомегоневрозакоторыйвтакомслучаеследуетопределит
ькакистероэпилепсиютоестькактяжелуюистериюутверждатьэтосполнойуверенность
юнельзяподвумпричинамвопервыхпотомучтодатыанамнезическихприпадковтакназыв
аемойэпилепсиидостоевскогонедостаточныиненадежныавовторыхпотомучтопониман
иесвязанныхсэпилептоиднымиприпадкамиболезненныхсостоянийостаетсянеясныма
', (13, 151))
```

# Успіх!

Ключ у нас (13, 151)