МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

"МИРЭА - Российский технологический университет"

РТУ МИРЭА

Институт Кибернетики

Базовая кафедра №252 - Информационной безопасности

ОТЧЁТ ПО УЧЕБНОЙ ПРАКТИКЕ

Тема практики: "Исследование элементарных шрифтов"(вариант №24)

Отчёт представлен к рассмотрению:
Студентка группы КККСО-03-19 «____» _____ 2020 г. _____ (подпись) Никишина А.А.

Отчёт утверждён.
Допущен к защите:
Руководитель практики «____» _____ 2020 г. _____ (подпись) Плешаков А.С.

Москва 2020

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

"МИРЭА - Российский технологический университет"

РТУ МИРЭА

Институт Кибернетики

Базовая кафедра №252 - Информационной безопасности

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА УЧЕБНУЮ ПРАКТИКУ

Обучающаяся	Никишина Анна Александровна
Шифр	19К0603
Специальность	Компьютерная безопасность (10.05.01)
Учебная группа	ККСО-03-19

1. Тема учебной практики: «Исследование элементарных шифров».

2. Содержание практики:

2.1. Изучение понятийного аппарата криптографии и криптографического анализа.

2.2. Исследование шифра простой замены.

2.3. Исследование криптосистемы Энигма.

3. Этапы учебной практики:

Номер этапа	Содержание этапа учебной практики	Результат выполнения этапа учебной практики	Срок выполнения
1	Изучение понятийного аппарата криптографии и криптографического анализа.	Формализация основных задач криптографии и криптографического анализа, глоссарий основных понятий. Описание алгебраической модели шифра. Классификация шифров по различным признакам.	12.03.2020
2	Исследование шифра простой замены.	Модель шифра простой замены и подходы к его анализу. Описание процесса поиска для данного закрытого текста, зашифрованного методом простой замены, соответствующего открытого текста.	09.04.2020
3	Исследование шифра «Энигма».	Описание процедуры зашифрования и расшифрования на конкретных текстах. Программная реализация Энигмы. Описание процесса определения ключа для известной пары открытого и закрытого текстов и его использования для расшифрования данного закрытого текста.	28.05.2020

3. Перечень разрабатываемых материалов:

3.1. Отчёт, в котором отражён ход проделанной работы.

3.2. Исходные коды разработанного программного обеспечения.

3.3. Презентационные материалы, демонстрирующие конечные результаты.

Руководитель практики:

«____» _____ 2020 г. _____ Плешаков А.С.
(подпись)

Задание получила:

«____» _____ 2020 г. _____ Никишина А.А.
(подпись)

Содержание

1. Изучение понятийного аппарата криптографии и криптоанализа.

1.1. Глоссарий основных понятий.

Криптография – это наука о способах преобразования информации с целью ее защиты от незаконных пользователей.

Открытый (исходный) текст — данные (не обязательно текстовые), передаваемые без использования криптографии или, другими словами, незашифрованные данные.

Шифротекст, шифрованный (закрытый) текст — данные, полученные после применения криптосистемы (обычно — с некоторым указанным ключом). Другое название криптограмма.

Шифр, криптосистема — семейство обратимых преобразований открытого текста в шифрованный. Ключ — параметр шифра, определяющий выбор конкретного преобразования данного текста. В современных шифрах криптографическая стойкость шифра целиком определяется секретностью ключа (принцип Керкгоффса). Также выделяют ключ шифрования (encription key) и ключ расшифрования (decryption key).

Шифрование — процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.

Расшифровывание — процесс нормального применения криптографического преобразования шифрованного текста в открытый.

Асимметричный шифр, двухключевой шифр, шифр с открытым ключом — шифр, в котором используются два ключа, шифрующий и расшифровыва-

ющий. При этом, зная лишь ключ зашифровывания, нельзя расшифровать сообщение, и наоборот.

Открытый ключ — тот из двух ключей асимметричной системы, который свободно распространяется. Шифрующий для секретной переписки и расшифровывающий — для электронной подписи.

Секретный ключ, закрытый ключ — тот из двух ключей асимметричной системы, который хранится в секрете. Криптоанализ — наука, изучающая математические методы нарушения конфиденциальности и целостности информации.

Криптоаналитик — учёный, создающий и применяющий методы криптоанализа.

Криптографическая атака — попытка криптоаналитика вызвать отклонения в атакуемой защищённой системе обмена информацией. Успешную криптографическую атаку называют взлом или вскрытие.

Дешифрование (дешифровка) — процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного. Термин дешифрование обычно применяют по отношению к процессу криптоанализа шифротекста (криптоанализ сам по себе, вообще говоря, может заключаться и в анализе криптосистемы, а не только зашифрованного ею открытого сообщения).

Криптографическая стойкость — способность криптографического алгоритма противостоять криптоанализу.

Имитозащита — защита от навязывания ложной информации. Другими словами, текст остаётся открытым, но появляется возможность проверить, что его не изменяли ни случайно, ни намеренно. Имитозащита достигается обычно

за счёт включения в пакет передаваемых данных имитовставки.

Имитовставка — блок информации, применяемый для имитозащиты, зависящий от ключа и данных.

Электронная цифровая подпись, или электронная подпись — асимметричная имитовставка (ключ защиты отличается от ключа проверки). Другими словами, такая имитовставка, которую проверяющий не может подделать.

Центр сертификации — сторона, чья честность неоспорима, а открытый ключ широко известен. Электронная подпись центра сертификации подтверждает подлинность открытого ключа.

Хеш-функция — функция, которая преобразует сообщение произвольной длины в число («свёртку») фиксированной длины. Для криптографической хеш-функции (в отличие от хеш-функции общего назначения) сложно вычислить обратную и даже найти два сообщения с общей хеш-функцией.

Гибридная криптосистема — это система шифрования, совмещающая преимущества криптосистемы с открытым ключом с производительностью симметричных криптосистем.

1.2. Основные задачи криптографии и криптографического анализа

Обеспечение конфиденциальности данных (предотвращение несанкционированного доступа к данным). Это одна из основных задач криптографии, для ее решения применяется шифрование данных, т.е. такое их преобразование, при котором прочитать их могут только законные пользователи, обладающие соответствующим ключом.

Обеспечение целостности данных — гарантии того, что при передаче или хранении данные не были модифицированы пользователем, не имеющим на это права. Под модификацией понимается вставка, удаление или подмена информации, а также повторная пересылка перехваченного ранее текста.

Обеспечение аутентификации. Под аутентификацией понимается проверка подлинности субъектов (сторон при обмене данными, автора документов, и т.д.) или подлинности самой информации. Частным случаем аутентификации является идентификация — процедура доказательства субъектом того, что он действительно является именно тем, за кого себя выдает. Во многих случаях субъект X должен не просто доказать свои права, но сделать это так, чтобы проверяющий субъект (Y) не смог впоследствии сам использовать полученную информацию для того, чтобы выдать себя за X. Подобные доказательства называются «доказательствами с нулевым разглашением».

Обеспечение невозможности отказа от авторства — предотвращение возможности отказа субъектов от совершенных ими действий (обычно — невозможности отказа от подписи под документом). Эта задача неотделима от двойственной — обеспечение невозможности приписывания авторства. Наиболее яркий пример ситуации, в которой стоит такая задача — подписание договора двумя или большим количеством лиц, не доверяющих друг другу. В такой ситуации все подписывающие стороны должны быть уверены в том, что в будущем, во-первых, ни один из подписавших не сможет отказаться от своей подписи и, во вторых, никто не сможет модифицировать, подменить или создать новый документ (договор) и утверждать, что именно этот документ был подписан. Основным способом решения данной проблемы является использовацифровой подписи.

Помимо перечисленных основных задач можно назвать также электронное голосование, жеребьевку, разделение секрета (распределение секретной информации между несколькими субъектами таким образом, чтобы воспользоваться ей они могли только все вместе) и многое другое.

1.3. Описание алгебраической модели шифра

Пусть T, C и K — конечные множества возможных открытых текстов, шифртекстов и ключей. Обычно каждое из этих множеств представляет собой множество слов в некотором алфавите, причем алфавиты открытых текстов, шифртекстов и ключей могут различаться. Для большинства современных систем шифрования открытые тексты, шифртексты и ключи представляют собой слова в алфавите 0,1, т.е. последовательности нулей и единиц. Процедура шифрования задает функцию $Ek : T \mapsto C$, которая отображает множество открытых текстов во множество шифртекстов в зависимости от некоторого ключа $k \in K$. Аналогично, процедура расшифрования $Dk : C \mapsto T$ также зависит от ключа k и отображает множество шифртекстов во множество открытых текстов. Так как получатель всегда должен иметь возможность по шифртексту восстановить исходный текст, то при любом k из K функции E_k и D_k должны удовлетворять условию: $D_k E_k = I$, где I — тождественное отображение T в T.

1.4. Классификация шифров по различным признакам

1.4.1. Симметричные системы шифрования

К симметричным системам шифрования относятся такие системы, в которых для шифрования и для расшифрования используется один и тот же ключ. Поэтому такие системы называют также одноключевыми.

- **Шифры замены**

Простейшим из шифров замены является одноалфавитная подставновка, называемая также шифром простой замены. Ключом такого шифра является взаимно однозначное отображение (подстановка) F алфавита открытого текста (X) в алфавит шифртекста (Y) : $F : X \leftrightarrow Y$. Зафиксируем нумерацию символов в алфавитах X и Y: X $= x_1, x_2, \ldots x_n$, Y $= y_1, y_2, \ldots y_n$. Тогда отображение F фактически задается перестановкой π порядка $n = |X| = |Y|$: при

шифровании символ x_i открытого текста заменяется на символ $\pi(i)$ у шифртекста. Эта перестановка может быть задана либо таблицей, либо с помощью формулы. При задании с помощью формулы значение $\pi(i)$ представляется в виде выражения, зависящего от i. Типичным примером шифра замены является шифр Цезаря. Этот шифр реализует следующее преобразование текста, записанного с помощью латинского алфавита: каждая буква открытого текста заменяется буквой, стоящей на три позиции позже нее в алфавите (при этом алфавит считается записанным по кругу).
Шифры простой замены в настоящее время не используются, поскольку их стойкость невелика. Методы взлома таких шифров основаны на анализе частотности отдельных символов и их комбинаций.

- **Шифры перестановки**

Ключом шифра перестановки является перестановка номеров символов открытого текста. Это, в частности, означает, что длина ключа шифрования должна быть равна длине преобразуемого текста. Для того чтобы из секретного ключа получить ключ шифрования, удобный для использования в шифрах перестановки, предложен ряд методов. С помощью одного из таких методов формируются так называемые маршрутные перестановки. Открытый текст записывают в некоторую геометрическую фигуру (чаще всего — прямоугольник) по некоторой траектории, а затем, выписывая символы из этой фигуры по другой траектории, получают шифртекст.

- **Гаммирование**

Формально гаммирование можно отнести к классу шифров многоалфавитной замены. Однако, благодаря удобству реализации и формального описания, шифры гаммирования широко используются, и обычно их выделяются в отдельный класс. Суть метода гаммирования заключается в следующем. С помощью секретного ключа k генерируется последовательность символов $g = g_1 g_2 \dots g_i \dots$, эта последовательность называется гаммой. При шифровании гамма накладывается на открытый текст $t = t_1 t_2 \dots t_i \dots$, т.е. символы шифртекста получаются из соответствующих символов открытого текста и гаммы с

помощью некоторой обратимой операции: $c_i = t_i \cdot g_i$, $i = 1, 2, \ldots$ В качестве обратимой операции обычно используется либо сложение по модулю количества букв в алфавите N : $c_i = t_i + g_i(modN)$, либо, при представлении символов открытого текста в виде двоичного кода, операция поразрядного суммирования по модулю 2 (операция 'побитовый XOR'): $c_i = t_i \bigoplus g_i$. Расшифрование осуществляется применением к символам шифртекста и гаммы обратной операции: $t_i = c_i \breve{} g_i(modN)$ или $t_i = c_i \bigoplus g_i$ (операция XOR является обратной к самой себе). Стойкость систем шифрования, основанных на гаммировании, зависит от характеристик гаммы — ее длины и равномерности распределения вероятностей появления знаков гаммы.

Наиболее стойким является гаммирование с бесконечной равновероятной случайной гаммой, т.е. процедура шифрования, удовлетворяющая следующим трем условиям, каждое из которых является необходимым:

1) все символы гаммы полностью случайны и появляются в гамме с равными вероятностями;

2) длина гаммы равна длине открытого текста или превышает ее;

3) каждый ключ (гамма) используется для шифрования только одного текста, а потом уничтожается.

Такой шифр не может быть взломан в принципе, то есть является абсолютно стойким. Однако абсолютно стойкие шифры очень неудобны в использовании, и поэтому почти не применяются на практике.

1.4.2. Асимметричные криптографические системы

В этих системах для обмена данными используются два ключа, один из которых является секретным, а другой — открытым, т.е. общедоступным. По этой причине асимметричные системы называются также двухключевыми. Все асимметричные криптографические системы основаны на использовании односторонних функций с секретом.

Односторонняя функция с секретом — это функция $Fk : X \to Y$, зависящая от параметра $k \in K$ (этот параметр называется секретом), для которой выполняются следующие условия:

1) при любом $k \in K$ существует эффективный алгоритм, вычисляющий $Fk(x)$ для любого $x \in X$;

2) при неизвестном k не существует эффективного алгоритма инвертирования функции Fk;

3) при известном k существует эффективный алгоритм инвертирования функции Fk.

2. Изучение шифра простой замены

2.1. Модель шифра простой замены и способы её реализации

Шифр простой замены – класс методов шифрования, сводящихся к созданию таблицы шифрования, в которой для каждого символа из открытого текста подбирается однозначный символ или набор символов из алфавита, составляющего зашифрованный текст. Реализация шифра простой замены означает создание такой таблицы, содержащей два алфавита:

- Нормативный алфавит. Он включает в себя все необходимые к зашифровке символы исходного текста. Например, для текста, написанного на кириллице, таким алфавитом будет последовательность А, Б, .., Я. Также допускается исключение из этого алфавита некоторых символов, например, «Ё», и различная шифровка для прописных и строчных букв.

- Шифровальный алфавит, состоящий из символов зашифрованного текста. Допускается, чтобы символы могли принадлежать одновременно двум алфавитам, однако, возможен пример замены «кириллица – расширенная латиница» или замена на любые другие символы или наборы символов. Единственное условие – одинаковая мощность обоих алфавитов. Данный факт обуславливается тем, что подстановка из одного алфавита в другой должна быть однозначна, или биективна.

  Рассмотрим пример шрифта простой замены.

♦ *Пример 2.1.*

Исходный текст «ЖИЗНЬ».
Нормативный алфавит: Ж, З, И, Н, Ь.
Выберем шифровальный алфавит: Б, Л, О, Ь, Ц.

Ж	З	И	Н	Ь
Б	Л	О	Ь	Ц

Таблица 2.1 – Пример подстановки шифра простой замены.

Значит, зашифрованное сообщение будет звучать как «БОЛЬЦ».

Как мы можем заметить, имея таблицу подстановки, можно легко расшифровать любое сообщение, зашифрованное таким образом. Однако, надёжность шифра простой замены гарантируется тем, что количество возможных вариантов подстановок, если гарантирован тот факт, что алфавиты шифра и открытого текстов равны, вычисляется по формуле $N = M!$, где M – мощность алфавита. Путём нехитрых подсчётов можно вычислить, что даже для нерасширенной латиницы такое число будет равно $26! = 4 \times 10^{26}$. Для кириллицы, расширенной латиницы и многих иных алфавитов число N будет ещё больше, что делает «ручной» подбор ключа для шифра простой замены практически невозможным.

2.2. История шифра простой замены и его разновидности

Один из древнейших и наиболее хорошо известных шифров простой замены – шифр Цезаря, используемый ещё в первом веке до нашей эры. Суть этого шифра заключается в том, что каждый символ открытого текста зашифровывается символом, сдвинутым в отношении него на некоторое число k по алфавиту исходного текста. Приведём пример такого шифра.

♦ *Пример 2.2.*

Исходный текст: «DEPRESSION».

Предположим, что k = 5. В таком случае таблица подстановок будет такой:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

V	W	X	Y	Z
A	B	C	D	E

Таблица 2.2 – Пример подстановки шифром Цезаря с k = 5

Тогда зашифрованное сообщение будет таким: «IJUWJXXNTS».

Успех шифра Цезаря был обеспечен в первую очередь тем, что большинство людей, способных перехватить донесения, были неграмотны, и считали, что послание написано на неизвестном иностранном языке. Однако сейчас такой шифр легко взламывается, пусть «метод грубой силы» и остаётся самым действенным для шифра Цезаря. Заключается он в том, что часть зашифрованного сообщения с алфавитом мощностью M сдвигается посимвольно по алфавиту от 1 до M-1. Затем по найденной подстановке составляется таблица по типу таблицы 2.2, и текст легко расшифровывается.

Математическая модель шифра Цезаря может примерно быть записана так:

$$y = (x + k) mod M$$
$$x = (y - k) mod M$$

, где y – символ зашифрованного текста, x – символ открытого текста, M – мощность алфавита, а k – ключ. Фактически, шифр Цезаря является частным случаем аффинного шифра.

Аффинный шифр – приблизительный ровесник шифра Цезаря, однако даёт гораздо большее пространство для творчества и гораздо большее количество возможных ключей. Он всё ещё является моноалфавитным шифром, однако уже более сложным. Реализация сводится к тому, что каждому символу алфавита ставится в соответствие некое число из диапазона от 0 до M – 1, а затем по специальной формуле вычисляется новое число, буквенное значение которой и заменит старый символ в тексте. Процесс шифрования можно описать следующей формулой:

$$E(x) = (ax + b) mod M$$

где x – номер шифруемого символа в алфавите, a и b – ключ шифрования, а M – размер алфавита.

Процесс дешифрования же описывается иной формулой:

$$D(x) = a^{-1}(x - b) mod M$$

, где a^{-1} – число, обратное a по модулю M. Также из этого исходит то, что для верной расшифровки число a должно быть взаимно простым с мощностью алфавита M. Рассмотрим латинский алфавит, в котором 26 букв. Всего чисел, меньших и взаимно простых с 26, 12. А именно: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25. Число b может принимать любое значение от 0 до 25, итого, всего максимально у нас может быть $12 \times 26 = 312$ различных вариантов ключа.

Говоря о шифрах простой замены, нельзя не упомянуть шифр атбаш, созданный повстанцами-израильтянами ессеями. Шифр до крайности прост, но смог вызвать достаточно крупную череду событий, связанных с ним. Суть шифра заключается в том, что буква исходного текста заменяется буквой под таким же номером, если идти с конца алфавита. (Само название атбаш состоит из букв «алеф», «тав», «бет» и «шин», то есть первой, последней, второй и предпоследней букв алфавита иврита). Математическая модель шифра примерно такова:

$$y = M - x + 1$$

, где y – символ зашифрованного текста, x – символ исходного, M – мощность алфавита.

Рассмотрим пример шифровки атбашем.

♦*Пример 2.3*

Шифруемое сообщение: «DEPRESSION».

Выпишем таблицу перевода для латинского алфавита:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F

V	W	X	Y	Z
E	D	C	B	A

Таблица 2.3 – Таблица атбаш для латиницы

Следовательно, зашифрованное сообщение будет звучать как «WVKIVHHRLM».

Криптоанализ шифра атбаш сводится к анализу частоты триграмм в тексте и в естественном языке.

2.3. Частотный анализ

Частотный анализ — основывается на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования.

Частотный анализ предполагает, что каждая буква алфавита того или иного языка в довольно длинном тексте встречается с определенной частотой, к примеру, для русского языка известно, что буквы «О», «П», «Р» встречаются очень часто, а вот «Й», «Ъ» — редко. К примеру, имеется зашифрованный текст, полученный методом какой-либо перестановки букв по определенному алгоритму, и аналитикам требуется его расшифровать. Для этого берется открытый текст, желательно довольно длинный, затем подсчитывается в нем частота каждой буквы, причем, чем больше будет текст, тем точнее получится расшифровка.

Следующий шаг – то же самое проделывается с зашифрованным текстом, подсчитывается частота каждого символа. Собственно говоря, весь процесс расшифровки сводится к тому, что сопоставляются частоты двух текстов. Например, в открытом тексте буква «О» встречается с частотой 33% , то есть от общего количества букв текста, буква «О» составляет 33%, а в зашифрованном

тексте с частотой 33% встречается буква «П», значит, с большей вероятностью под буквой «П» подразумевается «О».

2.4. Практический анализ зашифрованного текста

2.4.1. Подготовка к расшифровке текста

Проводя исследовательскую работу по учебной практике, мы провели расшифровку текста. Нам было известно, что текст имеет смысл, а так же, что он засекречен с помощью шифра простой замены.

Первым этапом в расшифровке текста, стало изучение базовых основ криптографии и понятий о засекречивании информации. Так же, в дальнейшем, нам с коллегой пригодились знания полученные на занятиях по основам программирования.

Следующим этапом стало начало написания программы для расшифровки текста. Выбрав тернистый путь изучения и расшифровки текста самостоятельно (без помощи готовых декодирующих ресурсов), мы составили математическую модель будущей программы, чтобы сразу иметь чёткое представление о её архитектуре и грамотно подойти к написанию и структурированию кода. Для написания нами был выбран язык программирования C, так как именно на этом языке программирования пересекаются наши с коллегой познания, а так же, в силу преподавания данного ЯП в нашем университете, навыки его использования были свежи как никогда.

После определения чёткой цели и постановки конкретных задач, используя материалы сайта Национального корпуса русского языка, мы получили частотный анализ символов русского языка. И имея все нужные составляющие, мы приступили к написанию программы.

Итак, по нашему мнению программа для раскрытия шифра простой замены, должна выполнять следующие функции:

1) Считывание закрытого текста.

2) Подсчёт символов в тексте.

3) Возможность считывания ключа с консоли.

4) Возможность редактирования ключа. непосредственно в коде программы (фича для ускорения отладки и подбора подстановки).

5) Наличие встроенного алфавита.

6) Частотный анализ текста.

7) Автоматическое создание и вывод открытого текста, путём автозамены символов из таблицы подстановок.

8) Сортировка таблицы подстановок.

9) Вывод в консоль данных о ходе выполнения программы.

2.4.2. Реализация алгоритмов расшифровки

Первая трудность, с которой мы столкнулись - это работа с файлами. Долгое время нам не удавалось воплотить в жизнь эту задумку. Перебрав все возможные причины ошибок при компиляции и проблем с отображением символов в терминале, мы, неожиданно для себя обнаружили, что причина кроется в том, что одна буква занимала 2 символа, из-за чего прежде нам не удавалось организовать корректную работу программы. Для скорейшего исправления этой помехи, мы с коллегой разделились и одна из нас продолжала работу над исходной программой с расширенным диапазоном возможностей, другая, разрабатывала аналогичную программу с меньшим количеством возможностей, но с сохранением базовых функций для расшифровки текста. К таким базовым функциям мы отнесли:

1) Частотный анализ. (результат в прил.1)

2) Подсчёт символов в тексте

3) Возможность редактирования ключа непосредственно в коде программы.

4) Автоматическое создание и вывод открытого теста.

5) Сортировк таблицы подстановок.

6) Вывод в консоль данных о ходе программы.

Начав работу "с двух фронтов нам удалось в ускоренные сроки создать расширенную программу, удобную для работы с известным ключом и более примитивную программу, отлично подходящую для подбора ключа.

После окончания работы над программной частью, мы с коллегой принялись за корректировку ключа - то бишь стандартного частотного анализа русского языка. Заменяя и выводя текст раз за разом нам удавалось повышать его читабельность и таким образом мы полностью подобрали ключ (результат в прил.2).Самой сложной частью оказались не знакомые нам всем с советских времён аббревиатуры, а фамилии персонажей, так как они были непредсказуемы.

Закончив с расшифровкой текста мы расставили пробелы и знаки препинания на своё усмотрение, после чего в сети интернет нашли исходный отрывок из книги и доработали пунктуацию.(результат в прил.3)

3. Исследование криптосистемы Энигма

3.1. История создания криптосистемы Энигма

«Энигма» — переносная шифровальная машина, использовавшаяся для шифрования и дешифрования секретных сообщений. Более точно, «Энигма» — целое семейство электромеханических роторных машин, применявшихся с 20-х годов XX века.

«Энигма» использовалась в коммерческих целях, а также военными службами во многих странах мира, но наибольшее распространение получила в нацистской Германии во время Второй мировой войны. Именно германская военная модель чаще всего является предметом дискуссий.

Впервые шифр «Энигмы» удалось дешифровать в польском Бюро шифров в декабре 1932 года. Четверо сотрудников разведки, Мариан Реевский, Ежи Ружицкий, Генрих Зыгальский и Иоганн Ревклид с помощью данных французской разведки, математической теории и методов обратной разработки смогли разработать специальное устройство для дешифровки закодированных сообщений, которое назвали криптологической бомбой. После этого немецкие инженеры усложнили устройство «Энигмы» и в 1938 году выпустили обновлённую версию, для дешифровки которой требовалось построить более сложные механизмы.

Во время Второй мировой войны в Англии для расшифровки сообщений, зашифрованных с помощью «Энигмы», была создана машина с кодовым названием «Turing Bombe», оказавшая значительную помощь антигитлеровской коалиции. Вся информация, полученная криптоанализом с её помощью, имела кодовое название «Ultra». Утверждалось, что это достижение являлось решающим фактором в победе союзников.

Несмотря на то, что с точки зрения современной криптографии шифр «Энигмы» был слаб, на практике только сочетание этого фактора с другими

(такими как ошибки операторов, процедурные изъяны, заведомо известный текст сообщений (например, при передаче метеосводок), захваты экземпляров «Энигмы» и шифровальных книг) позволили взломщикам шифров разгадывать шифры «Энигмы» и читать сообщения.

По приблизительным оценкам, было выпущено около 100 000 экземпляров шифровальных машин «Энигма».

3.2. Принципы работы Энигмы

Разберем принцип работы трехроторной Энигмы. В ней имелось три отсека для помещения трех роторов и дополнительный отсек для размещения рефлектора. Всего за время Второй мировой войны было изготовлено восемь роторов и четыре рефлектора, но одновременно могло использоваться ровно столько, на сколько была рассчитана машина. Каждый ротор имел 26 сечений, что соответствовало отдельной букве алфавита, а так же 26 контактов для взаимодействия с соседними роторами. Как только оператор нажимал на нужную букву, — замыкалась электрическая цепь, в результате чего появлялась шифрованная буква. Замыкание цепи происходило за счет рефлектора.

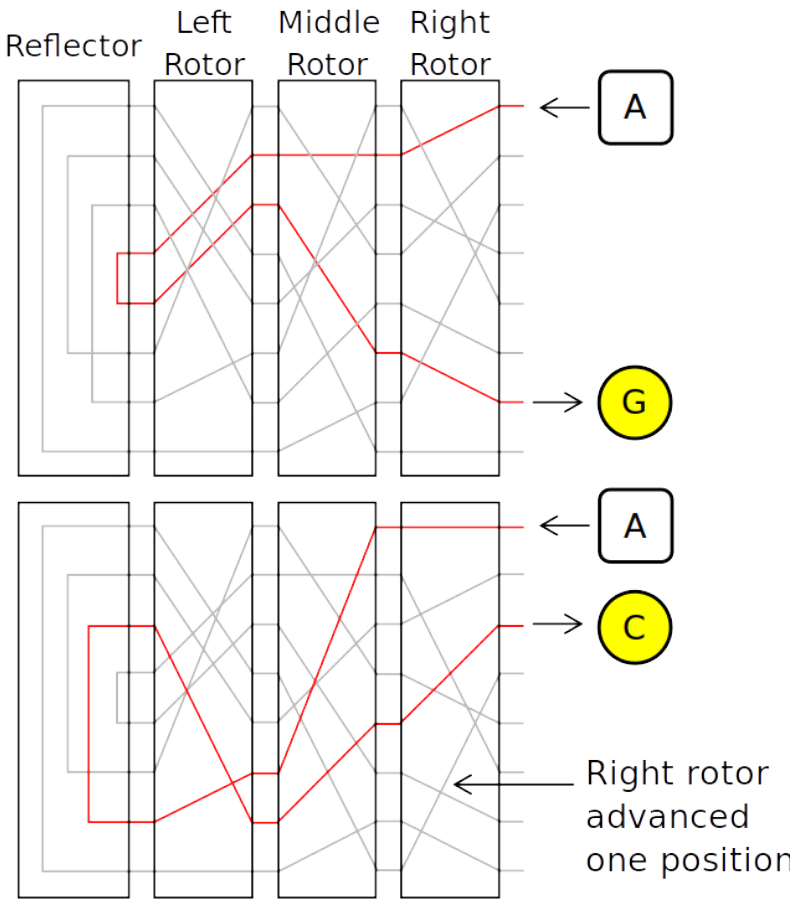

Рис.3.1 - Шифрующее действие Энигмы

На рисунке представлена иллюстрация нажатия клавиши «A» с последующей дешифрацией в букву «G». После ввода буквы крайний правый ротор перемещался вперед, меняя тем самым ключ. Так каким же образом одна букву заменялась на другую? Как я уже говорил, для Энигмы было разработано восемь различных роторов. Внутри каждого из них было установлено 26 различных коммутаций. Например, если на вход первого ротора поступала буква «N», то на выходе должна быть только «W» и никакая другая буква больше. Попади это буква на второй ротор, она бы уже преобразовалась в «T» и т.д. То есть, каждый ротор выполнял четко поставленную задачу в плане коммуникации. А какую же роль играли кольца? Рассмотрим следующий пример. Установим роторы III, II и I, а порядок колец «C», «U» и «Q».

Рис.3.2. - иллюстрация фронтального вида корпуса Энигмы

Нажмем на клавишу «A». Крайний правый ротор повернется вперед на один шаг, то есть, буква «Q» перейдет в «R». Ротор посередине также повернется вперед на букву «V», но об этом я расскажу чуть позже. Итак, наша буква «A» начинает путешествие с первого отсека, в котором установлен ротор I и на котором выставлена уже буква «R». Уже перед тем как попасть на первый ротор буква претерпевает свое первое преобразование, а именно: сложение с буквой «R» по модулю 26. Фактически, это шифр Цезаря. Если пронумеровать все буквы от 0 до 25, то буква «A» будет как раз таки нулевой. Значит, результатом сложения будет буква «R». Далее, мы с вами знаем, что в первом отсеке ротор I, а в его конструкции заложено, что буква «R» всегда переходит в «U». Теперь на очереди второй отсек с ротором II. Опять, перед попаданием на второй ротор, теперь уже буква «U» меняется по несколько иному алгоритму: к ней прибавляется разница значений последующего ротора и предыдущего. Поясню. На втором роторе ожидает нас буква «V», а на предыдущем, — «R», их разница равна четырем буквам, и именно они прибавляются к нашей букве «U». Поэтому, на второй ротор поступает буква «Y». Далее по

таблице находим, что во втором роторе букве «Y» соответствует «O». Далее опять смотрим разницу букв «C» и «V», — она равна семи. Значит, букву «O» сдвигаем на семь позиций и получаем «V». В роторе III «V» переходит в «M». Перед тем как попасть на рефлектор, из нашей буквы вычитается буква «C», преображая ее в букву «K». Далее происходит отражение. Если вы заметите, то в каждом роторе образуются большие циклические группы, например: (A – E – L – T – P – H – Q – X – R – U), а в рефлекторе они разбиты по парам: (A — Y)(B — R)(C — U) и т.д. Это сделано для того, чтобы потом это возможно было расшифровать. Предположим, что установлен рефлектор B, в котором «K» заменяется на «N» (и наоборот). Половина пути пройдена. Теперь мы опять прибавляем значение буквы «C», получив тем самым букву «P». Здесь наоборот, в строке третьего ротора находим «P» и смотрим, в при нажатии какой буквы она бы появилась. Это буква «H». Преобразование в третьем роторе закончено. Теперь из этой буквы вычитается разница букв «C» и «V», то есть семь. Получаем букву «A». Во втором роторе она переходит саму в себя, поэтому оставляем ее без изменений. Далее, вычитаем разницу букв «V» и «R», то есть четверку и получаем букву «W». В первом роторе её обратно преобразование отображается в букву «N». Остается только вычесть из нее букву «R» и получим искомую букву «W». Как видите, алгоритм работы машинки оказался не таким сложным каким казался. Для усовершенствования шифра немцы внедрили коммутационную панель, которая позволяла попарно менять местами буквы. Если мы соединим буквы «Q» и «W», то при вводе той же «A» мы получили бы «Q», так как по факту должна быть «W», но она заменена буквой «Q». Вот прилагаемая схема действия.

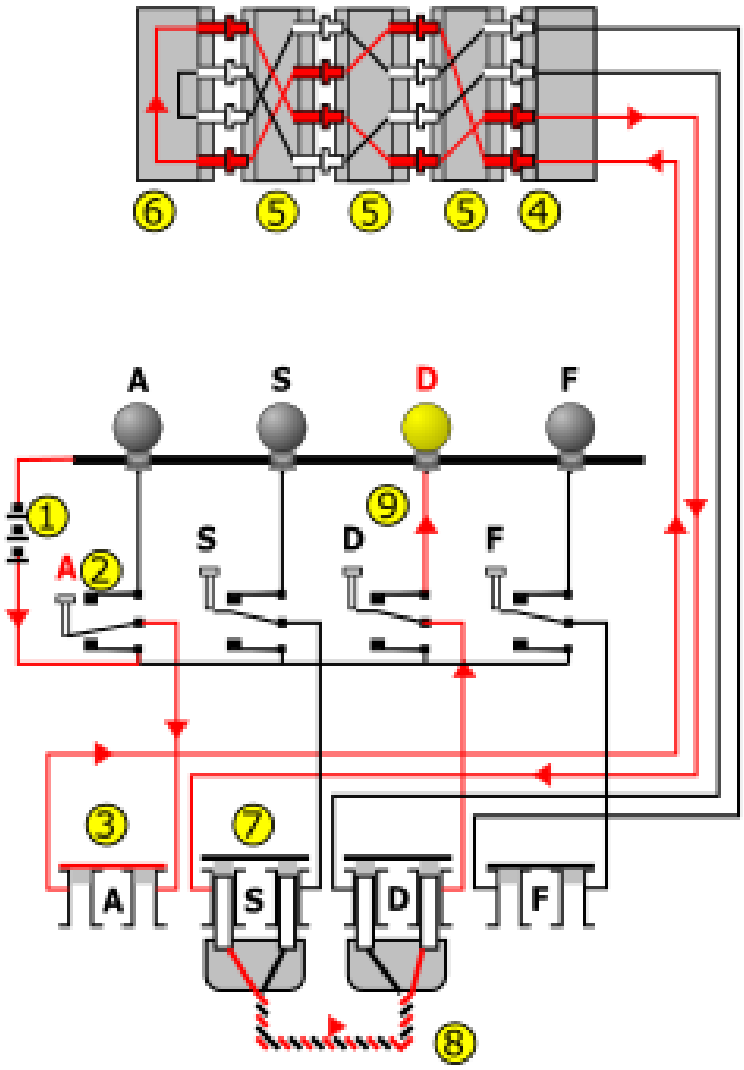

Рис.3.3 - Электрическая схема Энигмы, показывающая, куда течёт ток, когда буква «A» шифруется буквой «D»

3.3. Анализ стойкости Энигмы

Реальная Энигма отличалась от описанной демонстрационной машиной только в одном. А именно в устройстве роторов. В нашем примере ротор изменяет свое положение только при совершении полного оборота предыдущим диском. В настоящей Энигме каждый диск имел специальную выемку, которая в определенной позиции подцепляла следующий ротор и сдвигала его на одну позицию.

Расположение выемки для каждого из роторов можно было регулировать

с помощью специальных внешних колец. Начальное положение колец не влияло на коммутацию роторов и на результат шифрования отдельно взятой буквы, поэтому кольца не учитываются при расчете пространства ключей Энигмы.

Итак, базовая модель Энигмы имела 3 различных ротора, пронумерованных римскими цифрами I, II, III и реализующих следующие подстановки:
Entry = ABCDEFGHIJKLMNOPQRSTUVWXYZ
I = EKMFLGDQVZNTOWYHXUSPAIBRCJ
II = AJDKSIRUXBLHWTMCQGZNPYFVOE
III = BDFHJLCPRTXVZNYEIWGAKMUSQO
При шифровании роторы можно было располагать в любой последовательности, что для трех роторов дает 6 разных комбинаций. Помимо этого каждый ротор мог быть установлен в одной из 26 возможных стартовых позиций. Т.е. начальное положение роторов имеет всего 6*263=105456 комбинаций. Количество всех возможных соединений на коммутационной панели вычисляется по формуле:

$$\frac{n!}{((n-2m)!m!2^m)}$$

, где n — количество букв алфавита, m — количество соединенных пар.

Для 26 буква английского алфавита и 10 пар это составляет $150738274937250 = 2^{47}$ различных комбинаций.

Таким образом базовая версия Энигмы с тремя роторами имела солидное даже по современным меркам пространство ключей:
$150738274937250 * 105456 = 15896255521782636000 \approx 2^{64}$.

Такое огромное число вариантов внушало обманчивое чувство неуязвимости.

3.4. Криптоанализ Энигмы

Большое пространство ключей обеспечивает шифру Энигмы достаточно серьезный уровень стойкости к атакам по известному шифртексту.
Полный перебор 2^{64} вариантов даже на современных компьютерах дело не простое.
Однако все меняется если применить атаку с известным открытым текстом. Для такого случая существует весьма хитроумный метод, позволяющих пренебречь настройками коммутационной панели в процессе поиска ключевой комбинации, что сводит пространство ключей Энигмы всего к 105456 комбинациям и делает весь шифр фатально уязвимым.

Метод эксплуатирует наличие в паре открытый-закрытый текст так называемых «циклов». Чтобы объяснить понятие «цикл», рассмотрим следующее открытое сообщение P и соответствующий ему криптотекст C, зашифрованный Энигмой.
P = WETTERVORHERSAGEBISKAYA
C = RWIVTYRESXBFOGKUHQBAISE
Запишем каждый символ из пары в виде таблицы:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
w	e	t	t	e	r	v	o	r	h	e	r	s	a	g	e	b	i	s	k
r	w	i	v	t	y	r	e	s	x	b	f	o	g	k	u	h	q	b	a

21	22	23
a	y	a
i	s	e

Таблица 3.1 - подстановки реализуемые Энигмой

Обратите внимание на подстановки, реализуемые энигмой в 14, 15 и 20 позициях. На 14 шаге буква A шифруется в G. Последняя, в свою очередь, шифруется в K на 15 шаге. И затем буква K зашифровывается в A на 20 шаге, закольцовывая тем самым цепочку A-G-K-A. Такие закольцованные цепочки называются циклами. Наличие циклов позволяет разделить задачу взлома Энигмы на две простые составные части:

1) Поиск стартового положения роторов.

2) Поиск соединений коммутационной панели при известных установках роторов.

Мы знаем, что при шифровании в Энигме происходит несколько преобразований. Сперва сигнал проходит через коммутационную панель. Результат преобразования на коммутационной панели поступает в роторы. После чего сигнал попадает на рефлектор и возвращается через роторы на коммутационную панель, где выполняется последняя подстановка. Все эти операции можно представить математической формулой:
$E_i = S^{-1}R^{-1}TRS$, где S и S^{-1}, — преобразование на коммутационной панели на входе и выходе соответственно;
R и R^{-1} — преобразование в роторах на входе и выходе;
T — преобразование на рефлекторе.
Опустив коммутационную панель выразим внутреннее преобразование Энигмы через P_i :
$P_i = R^{-1}TR$
Теперь шифрование можно записать как:
$E_i = S^{-1}P_iS$

Используя формулу перепишем подстановки из примера в 14, 15 и 20 позициях.
$S^{-1}P_{14}S(A) = G$ или что одно и тоже $P_{14}S(A) = S(G)$.
$P_{15}S(G) = S(K)$
$P_{20}S(K) = S(A)$
Заменив в последнем выражении S(K) получим: $P_{20}P_{15}P_{14}S(A) = S(A)$ (1), где S(A) — буква, соединенная с A на коммутационной панели. Теперь атака сводится к тривиальному перебору всех возможных установок ротора. Для каждой комбинации роторов необходимо проверить выполнение равенства (1). Если равенство выполняется для буквы S, это означает что найдена правильная конфигурация роторов и что буква A соединена на коммутационной па-

нели с буквой S. Поиск остальных пар сводится к по буквенной расшифровке криптотекста и сопоставлению результата с известным открытым текстом.

Следует отметить, что с вероятностью $1/26$ равенство может выполняться и при неправильной установке роторов, поэтому для повышения надежности алгоритма желательно использовать несколько «циклов».

Еще один важный момент связан с тем, что атакующему может быть известна только часть зашифрованного сообщения. И в таком случае, прежде всего ему потребуется найти местоположение известного текста в полученной криптограмме. В решении этой задачи очень сильно помогает знание того факта, что Энигма никогда не шифрует букву саму в себя. Т.е. для нахождения правильного смещения нужно найти такую позицию в криптотексте при которой ни одна из букв закрытого текста не дублируется буквой открытого сообщения.

Список литературы

1) М. М. Глухов, В. П. Елизаров - «Алгебра» (2003)

2) Лев Лайнер - «Погоня за "Энигмой"» (2004)

3) Е. Б. Моховенко – «Теоретико-числовые методы криптографии» (2006)

4) Брюс Шнайер – «Практическая криптография» (2005)

5) Михаил Адаменко – «Основы классической криптографии. Секреты шифров и кодов» (2016)

6) Крис Эрнхард – «Квантовые вычисления для настоящих айтишников» (2020)

7) Брюс Шнайер – «Подстановочные шифры // прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си» (2002)

8) Материалы сайта www.habr.com

Приложения

Приложение 1.

Буква	Кол-во повторений	Частота
о	2893 раз.	11.02%
к	2380 раз.	9.07%
ц	1927 раз.	7.34%
з	1763 раз.	6.72%
б	1666 раз.	6.35%
ю	1661 раз.	6.33%
д	1400 раз.	5.33%
ь	1251 раз.	4.77%
у	1185 раз.	4.52%
е	1067 раз.	4.07%
ж	1013 раз.	3.86%
г	810 раз.	3.09%
ш	785 раз.	2.99%
э	768 раз.	2.93%
п	670 раз.	2.55%
л	555 раз.	2.11%
ч	515 раз.	1.96%
щ	464 раз.	1.77%
ъ	459 раз.	1.75%
с	435 раз.	1.66%
ф	428 раз.	1.63%
а	399 раз.	1.52%
н	309 раз.	1.18%
х	292 раз.	1.11%
в	248 раз.	0.94%
й	246 раз.	0.94%
я	175 раз.	0.67%
м	168 раз.	0.64%
и	101 раз.	0.38%
ё	89 раз.	0.34%
р	75 раз.	0.29%
ы	22 раз.	0.08%
т	4 раз.	0.02%

Приложение 2.

Таблица подстановки для ключа.

о	к	ц	з	б	ю	д	ь	у	е	ж	г	ш	э	п	л	ч	щ	ъ	с	ф	а	н	х
о	а	е	и	т	н	с	л	в	р	к	д	у	м	п	ь	ы	я	б	з	ч	г	ж	й

в	й	я	м	и	ё	р	ы	т
х	ш	ё	ю	э	щ	ц	ф	ъ

В верхней строке таблицы представлен топ букв по повторениям в закрытом тексте. А в нижней строке представлен откорректированный, под специфику текста, топ букв по повторениям в русском языке.

Приложение 3.

48.

Если не считать толстячка Густава с розовыми ушами, Доронин был на шарашке самым молодым зэком. Все сердца привлекал его необидчивый нрав, удатливость, быстрота. Немногие минуты, в которые начальство разрешало волейбол, Ростислав отдавался игре беззаветно; если стоящие у сетки пропускали мяч, он от задней черты бросался под него ласточкой, отбивал и падал на землю, в кровь раздирая колена и локти. Нравилось и необычное имя его Руська, вполне оправдавшееся, когда, через два месяца после приезда, его голова, бритая в лагере, заросла пышными русыми волосами. Его привезли из Воркутинских лагерей потому, что в учётной карточке ГУЛага он числился как фрезеровщик; на самом же деле оказался фрезеровщик липовый и вскоре был заменен настоящим. Но от обратной отсылки в лагерь Руську спас Двоетёсов, взявший его учиться на меньшем из вакуумных насосов.

Переимчивый Руська быстро научился. За шарашку он держался как за дом отдыха – в лагерях ему пришлось хлебнуть много бед, о которых он рассказывал теперь с весёлым азартом: как он доходил в сырой шахте, как стал делать себе мостырку- ежедневную температуру, нагревая обе подмышки камнями одинаковой массы, чтобы два термометра никогда не расходились

больше, чем на десятую долю градуса - двумя термометрами его хотели разоблачить. Но со смехом вспоминая своё прошлое, которое за двадцать пять лет его срока неотступно должно было повториться в будущем, Руська мало кому, и то по секрету, раскрывался в своем главном качестве донного парня, два года водившего за нос сыскной аппарат МГБ.

Достойный крестник этого учреждения, он так же не гнался за славой, как и оно. И так в пёстрой толпе обитателей шарашки он не был особо примечателен до одного сентябрьского дня. В этот день Руська с таинственным видом обошёл до двадцати самых влиятельных зэков шарашки, составлявших её общественное мнение, и с глазу на глаз каждому из них возбуждённо сообщил, что сегодня утром оперуполномоченный майор Шикин вербовал его в стукачи, и что он, Руська, согласился, предполагая использовать службу доносчика для всеобщего блага. Несмотря на то, что личное дело Ростислава Доронина было испещрено пятью сменёнными фамилиями, галочками, литерами и шифрами о его опасности, предрасположенности к побегу, о необходимости транспортировать его только в наручниках, майор Шикин в погоне за увеличением штата своих осведомителей счёл, что Доронин юноша, и потому нестоек, что он дорожит своим положением на шарашке и потому будет предан оперуполномоченному. Тайком вызванный в кабинет Шикина (вызывали, например, в секретариат, а там говорили: "да-да, зайдите к майору Шикину"), Ростислав просидел у него три часа. За это время, слушая нудные наставления и разъяснения кума, Руська своими зоркими ёмкими глазами изучил не только крупную голову майора, поседевшую за подшиванием доносов и кляуз, его черноватое лицо, его крохотные руки, его ноги в мальчиковых ботинках, мраморный настольный прибор и шёлковые оконные шторы, но и, мысленно переворачивая буквы, перечёл заголовки на папках и бумажки, лежавшие под стеклом, хотя сидел от края стола за полтора метра, и ещё успел прикинуть, какие документы Шикин, очевидно, хранит в сейфе, а какие запирает в столе. Порою Доронин простодушно уставлял свои голубые глаза в глаза майора и согласительно кивал. За этим голубым простодушием кипели самые отчаянные замыслы, но оперуполномоченный, привыкший к серому однообразию

людской покорности, не мог догадаться. Руська понимал, что Шикин действительно может услать его на Воркуту, если он откажется стать стукачом.

Не Руську одного, но всё поколение руськино приучили считать "жалость"чувством унизительным, "доброту"смешным, "совесть"выражением поповским. Зато внушали им, что доносительство есть и патриотический долг, и лучшая помощь тому, на кого доносишь, и содействует оздоровлению общества. Не то, чтоб это всё в Руську проникло, но и не осталось без влияния. И главным вопросом для него был сейчас не тот, насколько это дурно или позволительно стать стукачом, а что из этого получится? Уже обогащённый бурным жизненным опытом, множеством тюремных встреч и наслушавшись хлёстких тюремных споров, этот юноша не выпускал из виду и такую ситуацию, когда все эти архивы МГБ будут раскапывать, и всех тайных сотрудников предавать позорному суду. Поэтому согласиться на сотрудничество с кумом было в дальнем смысле так же опасно, как в ближнем отказаться от него.

Но кроме всех этих расчётов Руська был художник авантюризма. Читая занятные бумажки вверх ногами под настольным стеклом Шикина, он задрожал от предчувствия острой игры. Он томился от бездеятельности в тесном уюте шарашки! И для правдоподобия уточнив, сколько он будет получать, Руська с жаром согласился. После его ухода Шикин, довольный своей психологической проницательностью, прохаживался по кабинету и потирал одну крохотную ладонь о другую - такой осведомитель-энтузиаст обещал богатый урожай доносов. А в это самое время не менее довольный Руська обходил доверенных зэков и исповедывался им, что согласился быть стукачом из любви к спорту, из желания изучить методы МГБ и выявить подлинных стукачей. Другого подобного признания не помнили зэки, даже старые. Руську недоверчиво спрашивали зачем он, рискуя головой, похваляется. Он отвечал:

- А когда над этой сворой будет Нюрнбергский процесс, - вы за меня выступите свидетелями защиты.

Из двадцати узнавших зэков каждый рассказал ещё одному-двум, и никто не пошёл и не донёс куму! Уже одним этим полета людей утвердились выше подозрений. Событие с Руськой долго волновало шарашку. Мальчишке поверили. Верили ему и позже. Но, как всегда, у событий был свой внутренний ход. Шикин требовал материалов. Руське приходилось что-нибудь давать. Он обходил своих доверителей и жаловался:

- Господа воображаете, сколько стучат другие, если я вот месяца не служу, а как Шикин жмёт! Ну войдите в положение, подбросьте матерьяльчика!

Одни отмахивались, другие подбрасывали. Единодушно было решено погубить некую даму, которая работала из жадности, чтоб умножить тысячи, приносимые мужем. Она держалась с зэками презрительно, высказывалась, что их надо перестрелять, говорила она так среди вольных девушек, но зэкам быстро стало известно, и сама завалила двоих - одного на связи с девушкой, другого - на изготовлении чемодана из казённых материалов. Руська бессовестно оболгал её, что она берёт от зэков письма на почту и ворует из шкафа конденсаторы. И хотя он не представил Шикину ни одного доказательства, а муж дамы - полковник МВД, решительно протестовал, по неотразимой силе тайного доноса дама была уволена и ушла заплаканная. Иногда Руська стучал и на зэков - по каким-либо незлостным мелочам, сам же предупреждая их об этом. Потом перестал предупреждать, смолк. Не спрашивали и его. Невольно все поняли так, что он стучит и дальше, но уже о таком, в чём не признаешься. Так Руську постигла судьба двойников. Об игре его по-прежнему никто не донёс, но его стали сторониться. Рассказываемые им подробности, что у Шикина под стеклом лежит особое расписание, по которому стукачи заскакивают в кабинет без вызова, и по которому можно их ловить, как-то мало вознаграждали за его собственную принадлежность к причту стукачей. Не подозревал и Нержин, любящий Руську со всеми его интригами, что о Есенине на него стукнул тоже Руська. Потеря книги доставила Глебу боль, которой Руська предвидеть не мог. Тот рассудил, что книга Нержина собственная, это выяснится, отнять её никто не отнимет, а Шикина можно очень занять доно-

сом, что Нержин прячет в чемодане книгу, наверное принесенную ему вольной девушкой.

Ещё сохраняя на губах вкус клариного поцелуя, Руська вышел во двор. Снежная белизна лип была ему цветением, а воздух казался тёплым, как весной. В своих двухлетних скитаниях-скрываниях, все мальчишеские помыслы устремив на обман сыщиков, он совсем упустил искать любовь женщин. Он сел в тюрьму девственным, и от этого по вечерам ему было так безутешно-тяжело. Но, выйдя во двор, при виде низкого длинного штаба спецтюрьмы он вспомнил, что завтра в обед он здесь хотел задать спектакль. Подоспела как раз пора о том объявлять - раньше было нельзя, чтоб не сорвалось. И, овеянный восхищением Клары, оттого чувствуя себя втройне удачливым и умным, он огляделся, увидел Рубина и Нержина на краю прогулочного двора, и решительно направился к ним. Шапка его была сдвинута набок и назад, так что лоб весь и уголочек темени с космой волос были доверчиво открыты нехолодному дню. По строгому лицу Нержина, как видел Руська на подходе и потом по хмурому обёрнутому лицу Рубина, они говорили о серьёзном. Но Руську встретили незначительной подставной фразой, это было ясно. Что ж, сглотнув обиду, он толковал им:

- Надеюсь, вам известен общий принцип справедливого общества, что всякий труд должен быть оплачен? Так вот, завтра каждый Иуда будет получать свои серебренники за третий квартал этого года.

- Резинщики! - возмутился Нержин. - Уже и четвёртый отработали - а они только за третий? Почему такая задержка?

- Очень во многих местах надо подписывать платёжную ведомость, объяснял Руська извиняющимся тоном. В том числе буду получать и я.

- И тебе тоже платят за третий? - удивился Рубин. - Ведь ты же там служил только полквартала?

- Ну что ж, я - отличился! - с подкупающей открытой улыбкой оглядел обоих Руська.

- И прямо наличными?

- Боже упаси! Фиктивный денежный перевод по почте с зачислением суммы на лицевой счёт. Меня спросили: «От какого имени вам прислать? Хотите - от Ивана Ивановича Иванова?» Стандарт меня покоробил. Я попросил: «Нельзя ли от имени Клавы Кудрявцевой? Всё-таки приятно думать, что о тебе заботится женщина».

- И по сколько же за квартал?

- Вот тут-то самое остроумное! Осведомителю по ведомости выписывают сто пятьдесят рублей за квартал. Но надо для приличия переслать по почте, а неумолимая почта берёт три рубля почтовых сборов. Все кумовья настолько жадные, что своих денег добавить не хотят, и настолько ленивые, что не поднимут вопроса о повышении ставки сексотам на три рубля. Поэтому переводы будут все как один на 147 рублей. Поскольку нормальный человек никогда таких переводов не шлёт, эти недостающие тридцать гривенников и есть Иудина печать. Завтра в обед надо столпиться около штаба и у всех, выходящих от опера, смотреть перевод. Родина должна знать своих стукачей, как вы находите, господа?

49.

В этот самый час, когда отдельные редкие снежинки стали срываться с неба и падали на тёмную мостовую улицы Матросская Тишина, с булыжников которой скаты автомашин слизали последние остатки снега прошлых дней, в 318-й комнате студенческого городка на Стромынке шла предвечерняя воскресная жизнь девушек-аспиранток. 318-я комната на третьем этаже своим широким квадратным окном как раз и выходила на Матросскую Тишину, а от окна к

двери была продолговата, и вдоль стен её, справа и слева, упнулись по три железных кровати гуськом и шатко высились плетёные этажерки с книгами. Средней полосою комнаты, оставляя вдоль кроватей лишь узкие проходы, один за другим стояли два стола: ближе к окну - диссертационный, где громоздко теснились книги, тетради, чертежи и стопы машинописного текста, а дальше - общий, за которым сейчас Оленька гладила, Муза писала письмо, а Люда перед зеркалом раскручивала папильотки. У дверной стены ещё оставалось место для умывального таза, отгороженного занавеской. Умываться полагалось в конце коридора, но девушкам было там неуютно, холодно, далеко.

На кровати близ умывальника лежала венгерка Эржика и читала. Она лежала в халате, который в комнате назывался "бразильский флаг". У неё были ещё и другие затейливые халаты, восхищавшие девушек, но на выход она одевалась очень сдержанно, как бы даже стараясь не привлекать внимания. Она привыкла так за годы, когда была подпольщицей-коммунисткой в Венгрии.

Следующая в ряду постель Люды была растерзана (Люда не так давно встала одеяло) и простыня касались пола, зато поверх подушки и спинки кровати было бережно разложено уже выглаженное голубое шёлковое платье и чулки, и персидский коврик висел над кроватью. Сама же Люда за столом громко рассказывала историю ухаживания за ней некоего испанского поэта, вывезенного с родины ещё мальчиком. Она подробно вспоминала ресторанную обстановку, какой был оркестр, какие блюда, гарниры и пили что.

Утюг Оленьки был включён в патрон "жулик"над столом и оттуда свисал шнур. Чтобы не расходовали электричества, утюги и плитки были на Стромынке строго запрещены, розеток не ставили, а за "жуликами"охотилась вся комендатура. Оленька слушала Люду, посмеиваясь, но зорко занята была своей глажкой. Жакет этот и юбка к нему были её всё. Ей было бы легче прожечь утюгом себе тело, чем этот костюм. Оленька жила на одну аспирантскую стипендию, сидела на картошке и каше, если могла не доплатить в троллейбусе

двадцати копеек - не доплачивала, стена у её кровати была завешана географической картой - зато вот этот вечерний наряд был весь хорош, никакой части его не приходилось стыдиться.

Муза, избыточно-полная, с грубоватыми чертами лица и в очках старше своих тридцати лет, пыталась на столе, качаемом глажкой, и под этот назойливый оскорбляющий её рассказ, писать письмо. Попросить другого помолчать она вообще считала неделикатным. Останавливать же Люду было - её распалять, она бы только сдерзила. Люда была новая у них, не аспирантка, а приехала после финансового института на курсы политэкономов, да и приехала-то больше для развлечения. Отец её, генерал в отставке, много слал ей из Воронежа.

Люда была первобытно убеждена, что во встречах и вообще в отношениях с мужчинами состоит единственный смысл женской жизни. Но в сегодняшнем рассказе она выделяла ещё особую пикантность. У себя в Воронеже уже бывшая три месяца замужем и сходившаяся потом кой с какими другими мужчинами. Люда сожалела, что девичество у неё прошло как-то слишком мельком. И вот с первых же слов знакомства с испанским поэтом она разыгрывала начинающую, трепетала и стыдилась малейшего прикосновения к плечу или локтю, а когда потрясённый поэт вымолил у неё первый в её жизни поцелуй, она содрогалась, переходила от восторга к отчаянию и вдохновила поэта на стихотворение в двадцать четыре строки, к сожалению, не на русском.

Муза писала письмо своим глубоко-пожилым родителям в далёкий провинциальный город. Папа и мама её до сих пор любили друг друга как молодожёны, и всякое утро, идя на работу, папа до самого угла всё оборачивался и помахивал маме, а мама помахивала ему из форточки. И так же любила их дочь, и привыкла писать им часто и подробно о каждом своём переживании.

Но сейчас она не находила себя. Эти двое суток, с вечера последней пятницы, с Музой случилось такое, от чего затмилась её неутомимая повседневная

работа над Тургеневым - работа, заменявшая ей всякую другую жизнь, все виды жизни. Ощущение у неё было самое гадкое, будто она вымазалась во что-то грязное, позорное, чего нельзя ни отмыть, ни скрыть, ни показать - и существовать с этим тоже нельзя.

Случилось, что в эту пятницу вечером, когда она вернулась из библиотеки и собиралась ложиться, её вызвали в канцелярию общежития, а там сказали: "да, да, вот в эту, пожалуйста, комнату". А там сидели двое мужчин в штатском, вначале очень вежливых, представившихся ей как Николай Иваныч и Сергей Иваныч. Мало стесняясь поздним временем, они держали её час, и два, и три. Они начали с расспросов, с кем она в одной комнате, с кем на одной кафедре, хотя знали, конечно, не хуже её. Они неторопливо беседовали с ней о патриотизме, об общественном долге всякого научного работника не замыкаться в своей специальности, но служить своему народу всеми средствами, всеми возможностями. Против этого Муза не нашлась возразить, это было совершенно верно. Тогда братья Ивановичи предложили ей помогать им, то есть в определённое время встречаться с кем-нибудь из них в этой же вот канцелярии, или на агитпункте, или в клубных комнатах, а то и в самом университете, по уговору, и там отвечать на определённые вопросы или передавать свои наблюдения в письменном виде.

И с этого началось долгое, ужасное! Они стали говорить с ней всё грубее, покрикивать, обращаться уже на "ты": "Да что ты упрямишься? Тебя ж не иностранная разведка вербует!Нужна она иностранной разведке, как кобыле пятая нога..."Потом прямо заявили, что диссертацию защитить ей не дадут, а у неё шли последние месяцы, и диссертация была почти готова, научную карьеру ей поломают, потому что такие учёные хлюпики Родине не нужны. Это очень её напугало: разве был для них труд выгнать её из аспирантуры? Но тут они вынули пистолет, передавали друг другу и как бы невзначай держали наведенным на Музу. От пистолета у Музы, наоборот, страх миновал. Потому что в конце концов остаться живой, но выгнанной с чёрной характеристикой, было хуже. В час ночи Ивановичи отпустили её думать до вторника, вот до

ближайшего вторника, двадцать седьмого декабря, и взяли подписку о неразглашении.

Они уверяли, что им всё известно, и если она кому-нибудь расскажет об их разговоре, то по этой подписке будет тотчас арестована и осуждена.

Каким несчастным выбором они остановились именно на ней? Теперь обречённо она ждала вторника, не в силах заниматься, и вспоминала те недавние дни, когда можно было думать об одном Тургеневе, когда душу ничто не гнело, а она, глупая, не понимала своего счастья.

Оленька слушала с улыбкой, раз поперхнулась водой от смеха. Оленька хотя и поздновато из-за войны, в двадцать восемь лет была наконец счастлива-счастлива-счастлива и всем прощала всё, пусть каждый добывает себе счастье как может. У неё был возлюбленный, тоже аспирант, и сегодня вечером он должен был зайти за ней и увести.

- Я говорю: вы, испанцы, вы так высоко ставите честь человека, но если вы поцеловали меня в губы, то ведь я обесчещена!

Привлекательное, хотя и жестковатое лицо светловолосой Люды передало отчаяние обесчещенной девушки.

Худенькая Эржика всё это время, лёжа, читала "Избранное"Галахова. Эта книга раскрывала перед ней мир высоких светлых характеров, цельность которых поражала Эржику. Персонажей Галахова никогда не сотрясали сомнения - служить родине или не служить, жертвовать собой или не жертвовать. Сама Эржика по слабому знакомству с языком и обычаями страны ещё не видела таких людей тут, но тем более важно было узнавать их из книг.

И всё-таки она опустила книгу и перекатясь на бок, стала слушать также и Люду. Здесь, в 318-й комнате, ей приходилось узнавать противоположные

удивительные вещи: то инженер отказался ехать на увлекательное сибирское строительство, а остался в Москве продавать пиво, то кто-то защитил диссертацию и вообще не работает. Разве в Советском Союзе бывают безработные? То, будто, чтобы прописаться в Москве, надо дать большую взятку в милицию. "Но ведь это – явление моментальное? спрашивала Эржика. Она хотела сказать – временное.

Люда досказывала о поэте, что если выйдет за него замуж, то уж теперь ей нет выхода - надо правдоподобно изобразить, что она-таки была невинна. И стала делиться, как именно собирается представить это в первую ночь.

Змейка страдания прошла по лбу Музы. Неделикатно было бы открыто заткнуть пальцами уши. Она нашла повод отвернуться к своей кровати.

Оленька же весело воскликнула:

- Так героини мировой литературы совершенно зря каялись перед женихами и кончали с собой?

- Конечно ду-у-уры! - смеялась Люда. - А это так просто!

Вообще же Люда сомневалась, выходить ли за поэта:

- Он не член ССП, пишет всё на испанском, и как у него будет дальше с гонорарами? - ничего твёрдого!

Эржика была так поражена, что спустила ноги на пол.

- Как? - спросила она. - И ты... ив Советском Союзе тоже выходят замуж по счёту?

- Привыкнешь - поймёшь, - тряхнула Люда головой перед зеркалом. Все

папильотки уже были сняты, и множество белых завившихся локонов дрожало на её голове. Одного такого колечка было довольно, чтобы окольцевать юношу-поэта.

- Девочки, я делаю такое выведение... - начала Эржика, но заметила странный опущенный взгляд Музы на пол близ неё, и ахнула, и вздёрнула ноги на кровать.

- Что? Пробежала? - с искажённым лицом крикнула она.

Но девочки рассмеялись. Никто не пробежал. Здесь, в 318-й комнате, иногда даже и днём, а по ночам особенно нахально, отчётливо стуча лапами по полу и пища, бегали ужасные русские крысы. За все годы подпольной борьбы против Хорти ничего так не боялась Эржика, как теперь того, что эти крысы вскочат на её кровать и будут бегать прямо по ней. Днём ещё, при смехе подруг, страх её миновал, но по ночам она обтыкалась одеялом со всех сторон и с головой и клялась, что если доживёт до утра - будет уходить со Стромынки. Химичка Надя приносила яд, разбрасывали им по углам, они стихали на время, потом принимались за своё. Две недели назад колебания Эржики решились: не кто-нибудь из девочек, а именно она, зачерпывая утром воду из ведра, вытащила в кружке утонувшего крысёнка. Трясясь от омерзения, вспоминая его сосредоточенно-примирённую острую мордочку, Эржика в тот же день пошла в венгерское посольство и просила поселить её на частной квартире. Посольство запросило министерство иностранных дел СССР, министерство иностранных дел, министерство высшего образования, министерство высшего образования, ректора университета, тот - свою адмхозчасть, и хозчасть ответила, что частных квартир пока нет, жалоба же о якобы крысах на Стромынке поступает впервые. Переписка пошла в обратную сторону и снова в прямую. Всё же посольство обнадёживало Эржику, что комнату ей дадут.

Теперь Эржика, охватив подтянутые к груди колени, сидела в своём бразильском флаге как экзотическая птица.

- Девочки-девочки, - жалобным распевом говорила она. - Вы мне все так нравитесь! Я бы ни за что не ушла от вас мимо крыс.

Это была и правда и неправда. Девушки нравились ей, но ни одной из них Эржика не могла бы рассказать о своих больших тревогах, об одинокой на континенте Европы венгерской судьбе. После процесса Ласло Райка что-то непонятное творилось на её родине. Доходили слухи, что арестованы такие коммунисты, с кем она вместе была в подполье. Племянника Райка, тоже учившегося в МГУ, и ещё других венгерских студентов вместе с ним - отозвали в Венгрию, и ни от кого из них не пришло больше письма.

В запертую дверь раздался их условный стук "утюга не прячьте, свои!". Муза поднялась и, прихромнув (колено ныло у неё от раннего ревматизма), откинула крючок. Быстро вошла Даша - твёрдая, с большим кривоватым ртом.

- Девчёнки! Девчёнки! - хохотала она, но всё ж не забыла накинуть за собой крючок. - Еле от кавалера отвязалась! От кого? Догадайтесь!

- У тебя так жирно с кавалерами? - удивилась Люда, роясь в чемодане.

Действительно, университет отходил от войны как от обморока. Мужчин в аспирантуре было мало и всё какие-то не настоящие.

- Подожди! - Оленька вскинула руку и гипнотически смотрела на Дашу. - От Челюстей?

"Челюсти"был аспирант, заваливший три раза подряд диалектический и исторический материализмы и, как безнадёжный тупица, отчисленный из аспирантуры.

- От Буфетчика! - воскликнула Даша, стянула шапку-ушанку с плотно-

собранных тёмных волос и повесила её на колок. Она медлила снять дешёвенькое пальтецо с цыгеечным воротником, три года назад полученное по талону в университетском распределителе, и так стояла у двери.

- Ах - того?

- В трамвае еду - он заходит, смеялась Даша. - Сразу узнал. "Вам до какой остановки?"Ну, куда денешься, сошли вместе. "Вы теперь в той бане уже не работаете? Я заходил сколько раз - вас нет".

- А ты б сказала... - смех от Даши перебросился к Оленьке и охватывал её как пламя, - ты б сказала, ты б сказала! - Но никак она не могла выговорить своего предложения и, хохоча, опустилась на кровать, однако не мня разложенного там костюма.

- Да какой буфетчик? Какая баня? - добивалась Эржика.

- Ты б сказала! - надрывалась Оленька, но новые приступы смеха трясли её. Она вытянула руки и шевелением пальцев пыталась передать то, что не проходило через глотку.

Засмеялись и Люда, и ничего не понявшая Эржика, и сумрачное некрасивое лицо Музы разошлось в улыбке. Она сняла и протирала очки.

- Куда, говорит, идёте? Кто у вас тут, в студенческом городке? - хохотала и давилась Даша. - Я говорю, вахтёрша знакомая рукавички вяжет!

- Рукавички?

- Вяжет!

- Но я хочу знать! Но какой буфетчик? - умоляла Эржика.

Оленьку хлопали по хребту. Отсмеялись. Даша сняла пальто. В тугом свитере, в простой юбке с тесным поясом видно было, какая она гибкая, ладная, не устанет день нагибаться на любой работе. Отвернув цветистое покрывало, она осторожно присела на край своей кровати, убранной почти молитвенно, с особой взбитостью подушки и подушечки, с кружевной накидкой, с вышитыми салфеточками на стене. И рассказала Эржике:

- Это ещё осенью было, затепло, до тебя...Ну, где жениха искать? Через кого знакомиться? Людка и посоветовала: иди, мол, гулять в Сокольники, только одна! Девушкам всё портит, что они по двое ходят.

- Расчёт без промаха! - отозвалась Люда. Она осторожно стирала пятнышко с носка туфли.

- Вот я и пошла, - продолжала Даша, но уже без веселья в голосе. – Похожу, сяду, на деревья посмотрю. Действительно, подсел быстро какой-то, ничего по наружности. Кто же? Оказывается, буфетчик, в закусочной работает. А я где? Стыдно мне так стало, не сказать же, что аспирантка. Вообще учёная баба - страх для мужчин...

- Ну так не говори! Так можно чёрт знает до чего дойти! - недовольно возразила Оленька.

В мире, таком прореженном и таком опустевшем, после того как вытолкнули из него железное туловище войны, когда зияли только ямки чёрные в тех местах, где должны были двигаться и улыбаться их сверстники или старшие их на пять-на десять-на пятнадцать лет, этими неизвестно кем составленными, грубыми, никакого смысла не выражающими словами "учёная баба"нельзя же было захлопывать тот светлый яркий луч науки, который оставался их роковому женскому поколению на всякие личные неудачи.

- Сказала, что кассиршей в бане работаю. Пристал - в какой бане, да в какую смену. Еле ушла...

Всё оживление покинуло Дашу. Тёмные глаза её смотрели тоскливо.

Она весь день прозанималась в Ленинской библиотеке, потом несытно и невкусно пообедала в столовой и возвращалась домой в унынии перед незаполнимым воскресным вечером, не обещавшим ей ничего.

Когда-то, ещё в средних классах просторной бревенчатой школы в их селе, ей нравилось хорошо учиться. Потом радовало, что под предлогом института ей удалось отцепиться от колхоза и прописаться в городе. Но вот уж ей было много лет, училась она восемнадцать кряду, надоело ей учиться до ломоты в голове - а зачем она училась? Простая бабья радость - ребёнка родить, и вот не от кого, не для кого.

И, задумчиво покачиваясь, Даша в смолкнувшей комнате произнесла свою любимую поговорку:

- Нет, девчата, жизнь - не роман...

При их МТС есть агроном один. Пишет Даше, упрашивает. Но вот-вот станет она кандидатом наук, и вся деревня скажет: для чего ж училась девка? - за агронома вышла. Это и любая звеньевая может...А с другой стороны Даша чувствовала, что и кандидат наук она будет ненастоящий, стреноженный, скованный, что вузовская работа будет ей - неподъёмный заклятый клин, что и кандидатом не посмеет и не сумеет она проникнуть в те высшие свободные круги науки.

Идущих в науку женщин, их целую жизнь хвалили, хвалили, так напевали, так много им обещали - и тем жёстче было теперь упереться в глыбу лбом.

Ревниво досмотрев за развязной удачливой соседкой, Даша сказала:

- Людка! А ты - ноги помой, советую.

Люда осмотрелась:

- Ты думаешь?

В нерешительности вытащила спрятанную электроплитку и включила в "жулик"вместо утюга.

Какой-нибудь работой хотелось деятельной Даше отогнать кручину. Она вспомнила, что есть у неё новокупка из белья, не того размера, но пришлось брать, пока выбросили. Теперь, достав, она начала ушивать.

Так все стихли, и можно было бы наконец вникнуть по-настоящему в письмо. Но нет, оно не выписывалось! Муза перечитала последние написанные фразы, одно слово заменила, несколько неясных букв подвела... - нет, письмо не удавалось! В письме была ложь, и мама с папой сразу это почувствуют. Они поймут, что дочке плохо, что случилось что-то чёрное, но почему же Муза не пишет прямо? В первый раз почему она лжёт?

Если бы никого сейчас не было в комнате, Муза бы застонала громко. Она просто заревела бы вслух, и, может, хоть чуть бы полегчало. А так она бросила ручку и подперлась ладонями, скрывая лицо ото всех. Ведь - вот как это делается! - выбор целой жизни, и ни с кем нельзя посоветоваться! Ни у кого не найти помощи! - подписка о неразглашении! А во вторник опять предстать перед теми двумя, уверенными, знающими готовые слова, готовые повороты. Как хорошо было жить ещё позавчера! А теперь всё погибло. Потому что они ведь не уступят. Но и ты не уступишь. Как же можно рассуждать о гамлетовском и донкихотском началах в человеке - и всё время помнить, что ты -

доносчица, что у тебя есть кличка - Ромашка или какая-нибудь Трезорка, и что ты должна собирать материалы вот на этих девчёнок или на своего профессора?

Муза сняла с зажмуренных глаз слезы, стараясь незаметно.

- А где Надюшка? - спросила Даша.

Никто не отозвался. Никто не знал.

Но у Даши за шитьём пришла своя мысль поговорить сейчас о Наде:

- Как вы думаете, девочки, сколько можно? Ну, пропал без вести. Ну, пошёл пятый год после войны. Ну, уж кажется, можно бы и отсечь, а?

- Ах, что ты говоришь! Что ты говоришь! - со страданием воскликнула Муза и вскинула руки над головой. Широкие рукава её сероклетчатого платья скользнули к локтям, обнажая белые рыхловатые руки. - Только так и любят! Истинная любовь перешагивает гробовую доску!

Сочные чуть припухлые губы Оленьки отошли в косую складку:

- После гробовой доски? Это, Муза, что-то трансцендентное. Память, нежные воспоминания, - но любовь?

- Вот именно: если человека нет вообще - как же его любить? - вела своё Даша.

- Я б ей, если б могла, честное слово, сама бы похоронное извещение прислала: что убит, убит, убит и в землю закопали! - горячо высказалась Оленька. - Что за проклятая война - пять лет прошло, а она всё на нас дышит!

- Во время войны, - вмешалась Эржика, - очень многие загнались далеко, за океан. Может и он там, живой.

- Ну, вот это может быть, - согласилась Оля. - Так она может надеяться. Но вообще, у Надюши есть такая тяжёлая черта: она любит упиваться своим горем. И только своим. Ей без горя даже чего-то бы в жизни не хватало.

Даша ожидала, пока все отговорятся, и медленно проводила кончиком иголки по рубчику, словно оттачивала её. Она-то знала, заводя разговор, как сейчас их всех поразит.

- Так слушайте, девчёнки, - веско сказала она теперь. - Всё это нас Надюшка морочит, врёт. Ничего она не считает мужа мёртвым, ни на какой возврат из без вести она не надеется. Она просто знает, что муж её жив. И даже знает, где он.

Все оживились:

- Откуда ты взяла?

Даша победно смотрела на них. Давно уже за её редкую приглядчивость её прозвали в комнате следователем.

- Слушать надо уметь, девки! Хоть раз обмолвилась она о нём как о мёртвом? Не-а. Она даже "был"старается не говорить, а как-нибудь так, без "был"и без "есть". Ну, если без вести пропал, то хоть разочек-то можно о нём порассуждать как о мёртвом?

- Но что ж тогда с ним?

- Да неужели не ясно? - вскрикнула Даша, вовсе откладывая шитьё.

Нет, им не было ясно.

- Он жив, но бросил её! И ей стыдно в этом признаться! И придумала - "без вести".

- А вот в это поверю! в это поверю! - поддержала Люда, хлюпая за занавеской.

- Значит, она жертвует собой во имя его счастья! - воскликнула Муза. - Значит, почему-либо нужно, чтоб она молчала и не выходила замуж!

- Тогда чего ей ждать? - не понимала Оленька.

- Да всё правильно, молодец Дашка! - выскочила Люда из-за занавески без халата, в одной сорочке, голоногая, отчего казалась ещё стройней и выше. - Заело её, потому и придумала, что - святоша, что верна мёртвому. Ни черта она не жертвует, дрожит она, чтоб кто-нибудь её приласкал, да никто её не хочет! Вот бывает так, ты будешь идти - на тебя все на улице будут оглядываться, а она хоть сама прилипай - а никому не нужна.

И ушла за занавеску.

- А к ней Щагов ходит, - сказала Эржика, с трудом выговаривая "щ".

- Ходит - это ещё ничего не значит! - уверенно отбивала невидимая Люда. - Надо, чтобы клюнул!

- Как это "клюнул"? - не поняла Эржика.

Рассмеялись.

- Нет, вы скажите так, - гнула Даша своё. - Может, она ещё надеется

отбить мужа у той назад?

В дверь раздался тот же условный стук - "утюга не прячьте, свои".

Все замолчали. Даша откинула крючок.

Вошла Надя - волочащимся шагом, с вытянутым постарелым лицом, как бы желая своим видом подтвердить все худшие насмешки Люды. Странно, она даже не обратилась к присутствующим ни с каким вежливо-приличным словом, не сказала "вот и я"или "ну, что тут нового, девочки?". Она повесила шубу и молча прошла к своей кровати.

Эржика снова читала. Муза опять убрала лицо в ладони. Оленька укрепляла розовые пуговицы на своей кремовой блузке.

Никто не нашёлся ничего сказать. Желая сгладить неловкость тишины, Даша протянула, будто заканчивая:

- Так что, девчата, жизнь - не роман...