Вар № 1

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 9797$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A, $e_A = 97$, $d_A = 6433$ соответственно. Открытый ключ абонента B, $e_B = 131$. Чему равен результат дешифрования зашифрованного сообщения $Y = 3025$, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль $P = 311$, образующий множества ненулевых вычетов по модулю P $\alpha = 17$, секретный ключ $a = 19$, случайно выбираемое число (рандомизатор) $r = 41$, найти зашифрованное сообщение Y, шифруемого сообщения $X = 27$.

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если $m=1$, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111110111 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 2

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования N = 11857 у всех абонентов один и тот же. Открытый и секретный ключи абонента A, $e_A = 159$, $d_A = 8039$ соответственно. Открытый ключ абонента B, $e_B = 211$. Чему равен результат дешифрования зашифрованного сообщения Y = 5494, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 313, образующий множества ненулевых вычетов по модулю P $\alpha = 10$, секретный ключ a = 17, случайно выбираемое число (рандомизатор) r = 52, найти зашифрованное сообщение Y, шифруемого сообщения X = 54.

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111110110 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 3

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования N = 10001 у всех абонентов один и тот же. Открытый и секретный ключи абонента A, $e_A = 341$, $d_A = 6461$ соответственно. Открытый ключ абонента B, $e_B = 193$. Чему равен результат дешифрования зашифрованного сообщения Y = 3850, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 337, образующий множества ненулевых вычетов по модулю P $\alpha = 10$, секретный ключ a = 16 , случайно выбираемое число (рандомизатор) r = 65, найти зашифрованное сообщение Y, шифруемого сообщения X = 39.

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111110101 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 4

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования N = 10541 у всех абонентов один и тот же. Открытый и секретный ключи абонента A, $e_A = 113$, $d_A = 7589$ соответственно. Открытый ключ абонента B, $e_B = 257$. Чему равен результат дешифрования зашифрованного сообщения Y = 8631, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 409, образующий множества ненулевых вычетов по модулю P $\alpha = 21$, секретный ключ a = 18 , случайно выбираемое число (рандомизатор) r = 42 , найти зашифрованное сообщение Y, шифруемого сообщения X = 79.

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111110100 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 5

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования N = 12193 у всех абонентов один и тот же. Открытый и секретный ключи абонента A, $e_A=141$, $d_A=7045$ соответственно. Открытый ключ абонента B, $e_B = 111$. Чему равен результат дешифрования зашифрованного сообщения Y = 1354, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 367, образующий множества ненулевых вычетов по модулю P $\alpha = 6$, секретный ключ a = 21, случайно выбираемое число (рандомизатор) r = 39, найти зашифрованное сообщение Y, шифруемого сообщения X = 248.

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111110011 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 6

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 9797$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A, $e_A = 211$, $d_A = 91$ соответственно. Открытый ключ абонента B, $e_B = 12$. Чему равен результат дешифрования зашифрованного сообщения $Y = 3504$, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль $P = 439$, образующий множества ненулевых вычетов по модулю P $\alpha = 15$, секретный ключ $a = 22$, случайно выбираемое число (рандомизатор) $r = 83$, найти зашифрованное сообщение Y, шифруемого сообщения $X = 234$.

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111110010 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 7

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 7031$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A, $e_A = 199$, $d_A = 2311$ соответственно. Открытый ключ абонента B, $e_B = 211$. Чему равен результат дешифрования зашифрованного сообщения $Y = 6235$, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль $P = 457$, образующий множества ненулевых вычетов по модулю P $\alpha = 13$ секретный ключ $a = 23$, случайно выбираемое число (рандомизатор) $r = 72$, найти зашифрованное сообщение Y, шифруемого сообщения $X = 69$.

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111101111 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 8

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования N = 589 у всех абонентов один и тот же. Открытый и секретный ключи абонента A, $e_A = 229$, $d_A = 1529$ соответственно. Открытый ключ абонента B, $e_B = 193$. Чему равен результат дешифрования зашифрованного сообщения Y = 1640, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 383, образующий множества ненулевых вычетов по модулю P $\alpha = 5$, секретный ключ a = 26, случайно выбираемое число (рандомизатор) r = 91, найти зашифрованное сообщение Y, шифруемого сообщения X = 123.

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111100100 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 9

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 8137$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A, $e_A = 197$, $d_A = 5129$ соответственно. Открытый ключ абонента B, $e_B = 679$. Чему равен результат дешифрования зашифрованного сообщения $Y = 6151$, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль $P = 241$, образующий множества ненулевых вычетов по модулю P $\alpha = 7$, секретный ключ $a = 28$, случайно выбираемое число (рандомизатор) $r = 54$, найти зашифрованное сообщение Y, шифруемого сообщения $X = 87$.

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111101000 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 10

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования N = 6497 у всех абонентов один и тот же. Открытый и секретный ключи абонента A, $e_A = 235$, $d_A = 5636$ соответственно. Открытый ключ абонента B, $e_B = 101$. Чему равен результат дешифрования зашифрованного сообщения Y = 2766, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 643, образующий множества ненулевых вычетов по модулю P $\alpha = 11$, секретный ключ a = 15, случайно выбираемое число (рандомизатор) r = 82, найти зашифрованное сообщение Y, шифруемого сообщения X = 49.

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111100100 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 11

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 10961$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 97$,$d_A = 1441$ соответственно. Открытый ключ абонента B, $e_B = 139$. Чему равен результат дешифрования зашифрованного сообщения Y = 9507, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 359 , образующий множества ненулевых вычетов по модулю P $\alpha = 7$, секретный ключ a = 27 , случайно выбираемое число (рандомизатор) r = 79 , найти зашифрованное сообщение Y, шифруемого сообщения X = 157 .

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111011010 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 12

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 11573$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 103$,$d_A = 7927$ соответственно. Открытый ключ абонента B, $e_B = 97$. Чему равен результат дешифрования зашифрованного сообщения Y = 7168, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 271 , образующий множества ненулевых вычетов по модулю P $\alpha = 6$, секретный ключ a = 31 , случайно выбираемое число (рандомизатор) r = 81 , найти зашифрованное сообщение Y, шифруемого сообщения X = 135 .

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111011001 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 13

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 9563$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 343$,$d_A = 2647$ соответственно. Открытый ключ абонента B, $e_B = 347$. Чему равен результат дешифрования зашифрованного сообщения Y = 8324, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 719 , образующий множества ненулевых вычетов по модулю P α = 11 , секретный ключ a = 25 , случайно выбираемое число (рандомизатор) r = 76 , найти зашифрованное сообщение Y, шифруемого сообщения X = 188 .
Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111011000 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 14

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 9379$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 131$,$d_A = 1963$ соответственно. Открытый ключ абонента B, $e_B = 257$. Чему равен результат дешифрования зашифрованного сообщения Y = 2846, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 479 , образующий множества ненулевых вычетов по модулю P α = 13 , секретный ключ a = 29 , случайно выбираемое число (рандомизатор) r = 93 , найти зашифрованное сообщение Y, шифруемого сообщения X = 177 .
Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111010111 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 15

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 11303$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 97$,$d_A = 4801$ соответственно. Открытый ключ абонента B, $e_B = 139$. Чему равен результат дешифрования зашифрованного сообщения Y = 9101, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 499 , образующий множества ненулевых вычетов по модулю P $\alpha = 7$, секретный ключ a = 20 , случайно выбираемое число (рандомизатор) r = 97 , найти зашифрованное сообщение Y, шифруемого сообщения X = 122 .

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111010010 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 16

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 9797$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 97$,$d_A = 6433$ соответственно. Открытый ключ абонента B, $e_B = 131$. Чему равен результат дешифрования зашифрованного сообщения Y = 3025, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 311 , образующий множества ненулевых вычетов по модулю P α = 17 , секретный ключ a = 19 , случайно выбираемое число (рандомизатор) r = 41 , найти зашифрованное сообщение Y, шифруемого сообщения X = 27 .
Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111010001 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 17

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 11857$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 159$,$d_A = 8039$ соответственно. Открытый ключ абонента B, $e_B = 211$. Чему равен результат дешифрования зашифрованного сообщения Y = 5494, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 313 , образующий множества ненулевых вычетов по модулю P α = 10 , секретный ключ a = 17 , случайно выбираемое число (рандомизатор) r = 52 , найти зашифрованное сообщение Y, шифруемого сообщения X = 54 .
Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111010000 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 18

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 10001$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 341$,$d_A = 6461$ соответственно. Открытый ключ абонента B, $e_B = 193$. Чему равен результат дешифрования зашифрованного сообщения Y = 3850, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 337 , образующий множества ненулевых вычетов по модулю P α = 10 , секретный ключ a = 16 , случайно выбираемое число (рандомизатор) r = 65 , найти зашифрованное сообщение Y, шифруемого сообщения X = 39 .
Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111001101 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 19

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 10541$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 113$,$d_A = 7589$ соответственно. Открытый ключ абонента B, $e_B = 257$. Чему равен результат дешифрования зашифрованного сообщения Y = 8631, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 409 , образующий множества ненулевых вычетов по модулю P α = 21 , секретный ключ a = 18 , случайно выбираемое число (рандомизатор) r = 42 , найти зашифрованное сообщение Y, шифруемого сообщения X = 79 .
Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111001100 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 20

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 12193$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 141$,$d_A = 7045$ соответственно. Открытый ключ абонента B, $e_B = 111$. Чему равен результат дешифрования зашифрованного сообщения Y = 1354, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 367 , образующий множества ненулевых вычетов по модулю P $\alpha = 6$, секретный ключ $a = 21$, случайно выбираемое число (рандомизатор) $r = 39$, найти зашифрованное сообщение Y, шифруемого сообщения $X = 248$.

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111001010 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 21

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 9797$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 211$,$d_A = 91$ соответственно. Открытый ключ абонента B, $e_B = 121$. Чему равен результат дешифрования зашифрованного сообщения Y = 3504, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 439 , образующий множества ненулевых вычетов по модулю P α = 15 , секретный ключ a = 22 , случайно выбираемое число (рандомизатор) r = 83 , найти зашифрованное сообщение Y, шифруемого сообщения X = 234 .
Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111001001 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 22

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 7031$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 199$,$d_A = 2311$ соответственно. Открытый ключ абонента B, $e_B = 211$. Чему равен результат дешифрования зашифрованного сообщения Y = 6235, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 457 , образующий множества ненулевых вычетов по модулю P α = 13 , секретный ключ a = 23 , случайно выбираемое число (рандомизатор) r = 72 , найти зашифрованное сообщение Y, шифруемого сообщения X = 69 .
Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111001000 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 23

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 5893$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 229$,$d_A = 1529$ соответственно. Открытый ключ абонента B, $e_B = 193$. Чему равен результат дешифрования зашифрованного сообщения Y = 1640, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 383 , образующий множества ненулевых вычетов по модулю P $\alpha = 5$, секретный ключ a = 26 , случайно выбираемое число (рандомизатор) r = 91 , найти зашифрованное сообщение Y, шифруемого сообщения X = 123 .

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111000111 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 24

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 8137$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 197$,$d_A = 5129$ соответственно. Открытый ключ абонента B, $e_B = 679$. Чему равен результат дешифрования зашифрованного сообщения Y = 6151, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 241 , образующий множества ненулевых вычетов по модулю P $\alpha = 7$, секретный ключ a = 28 , случайно выбираемое число (рандомизатор) r = 54 , найти зашифрованное сообщение Y, шифруемого сообщения X = 87 .

Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111000110 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.

Вар № 25

1. Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: $X = \{x_0, x_1\}$, $Y = \{y_0, y_1, y_2\}$, $K = \{k_0, k_1, k_2\}$. Зашифрование открытого текста x_i на ключе k_j дает зашифрованный текст y_m, где $m=(i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.

2. В сети абонентов, использующих систему RSA, модуль шифрования $N = 6497$ у всех абонентов один и тот же. Открытый и секретный ключи абонента A , $e_A = 235$,$d_A = 5636$ соответственно. Открытый ключ абонента B, $e_B = 101$. Чему равен результат дешифрования зашифрованного сообщения Y = 2766, отправленного в адрес абонента B, абонентом A, при атаке со стороны абонента A на секретный ключ абонента B?

3. При использовании шифра Эль-Гамаля с параметрами модуль P = 643 , образующий множества ненулевых вычетов по модулю P α = 11 , секретный ключ a = 15 , случайно выбираемое число (рандомизатор) r = 82 , найти зашифрованное сообщение Y, шифруемого сообщения X = 49 .
Полученное зашифрованное сообщение проверить посредством его расшифрования.

4. Назовем сеансовый ключ итеративного t-раундового блочного шифра m-слабым, если набор из t раундовых ключей содержит только m различных ключей, $1 \le m < t$. Если m=1, то такой сеансовый ключ называют слабым. Сколько слабых ключей в DES? Сколько слабых и 2-слабых ключей в Гост 28147-89? После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния?

5. Для двоичной последовательности 111000101 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига.