Шифры

В.А. Кириченко*

*Факультет математики и Лаборатория алгебраической геометрии и её приложений,
Национальный исследовательский университет Высшая школа экономики
и
Институт проблем передачи информации им. Харкевича РАН

Иннополис, июль 2018 г.

NATIONAL RESEARCH
UNIVERSITY

Программа

1. Шифры заменой

Как они устроены, и почему их легко разгадать

2. Шифры-решётки

Удобный шифр с ключом, который сложно разгадать

3. Шифры с открытым ключом

Как сделать шифры более стойкими за счёт асимметрии

4. Что почитать о шифрах

Книга Я.И.Перельмана “Живая математика” и статья С.А.Дориченко “Стойкие шифры”

Программа

1. Шифры заменой

Как они устроены, и почему их легко разгадать

2. Шифры-решётки

Удобный шифр с ключом, который сложно разгадать

3. Шифры с открытым ключом

Как сделать шифры более стойкими за счёт асимметрии

4. Что почитать о шифрах

Книга Я.И.Перельмана “Живая математика” и статья С.А.Дориченко “Стойкие шифры”

Программа

1. Шифры заменой

Как они устроены, и почему их легко разгадать

2. Шифры-решётки

Удобный шифр с ключом, который сложно разгадать

3. Шифры с открытым ключом

Как сделать шифры более стойкими за счёт асимметрии

4. Что почитать о шифрах

Книга Я.И.Перельмана “Живая математика” и статья С.А.Дориченко “Стойкие шифры”

Программа

1. Шифры заменой

Как они устроены, и почему их легко разгадать

2. Шифры-решётки

Удобный шифр с ключом, который сложно разгадать

3. Шифры с открытым ключом

Как сделать шифры более стойкими за счёт асимметрии

4. Что почитать о шифрах

Книга Я.И.Перельмана “Живая математика” и статья С.А.Дориченко “Стойкие шифры”

Шифры заменой

Как работают?

Каждая буква алфавита заменяется на другую букву (или символ)

Пример

Заменим букву А на букву Б, букву Б — на букву В, букву В — на букву Г и так далее. Букву Я заменим на букву А.

Задача

Расшифруйте слово ФОЙГЁСТЙУЁУ

Недостатки

Легко разгадать, даже не зная правила замены

Шифры заменой

Как работают?

Каждая буква алфавита заменяется на другую букву (или символ)

Пример

Заменим букву А на букву Б, букву Б — на букву В, букву В — на букву Г и так далее. Букву Я заменим на букву А.

Задача

Расшифруйте слово ФОЙГЁСТЙУЁУ

Недостатки

Легко разгадать, даже не зная правила замены

Шифры заменой

Как работают?

Каждая буква алфавита заменяется на другую букву (или символ)

Пример

Заменим букву А на букву Б, букву Б — на букву В, букву В — на букву Г и так далее. Букву Я заменим на букву А.

Задача

Расшифруйте слово ФОЙГЁСТЙУЁУ

Недостатки

Легко разгадать, даже не зная правила замены

Шифры заменой

Как работают?

Каждая буква алфавита заменяется на другую букву (или символ)

Пример

Заменим букву А на букву Б, букву Б — на букву В, букву В — на букву Г и так далее. Букву Я заменим на букву А.

Задача

Расшифруйте слово ФОЙГЁСТЙУЁУ

Недостатки

Легко разгадать, даже не зная правила замены

Решаем задачу

Зашифрованное слово

ФОЙГЁСТЙУЁУ

Шифр Юлия Цезаря

Зашифрованное изречение

Yhql, ylgl, ylfl

Шифр Юлия Цезаря

Зашифрованное изречение

Yhql, ylgl, ylfl

Перевод

Пришёл, увидел, победил

Расшифровка

Veni, vidi, vici

Шифр Юлия Цезаря

Зашифрованное изречение

Yhql, ylgl, ylfl

Перевод

Пришёл, увидел, победил

Расшифровка

Veni, vidi, vici

Шифр Юлия Цезаря

Зашифрованное изречение

Yhql, ylgl, ylfl

Перевод

Пришёл, увидел, победил

Расшифровка

Veni, vidi, vici

Шифр Юлия Цезаря

Зашифрованное изречение

Yhql, ylgl, ylfl

Перевод

Пришёл, увидел, победил

Расшифровка

Veni, vidi, vici

Шифр Юлия Цезаря

Зашифрованное изречение

Yhql, ylgl, ylfl

Перевод

Пришёл, увидел, победил

Расшифровка

Veni, vidi, vici

Шифр Юлия Цезаря

Зашифрованное изречение

Yhql, ylgl, ylfl

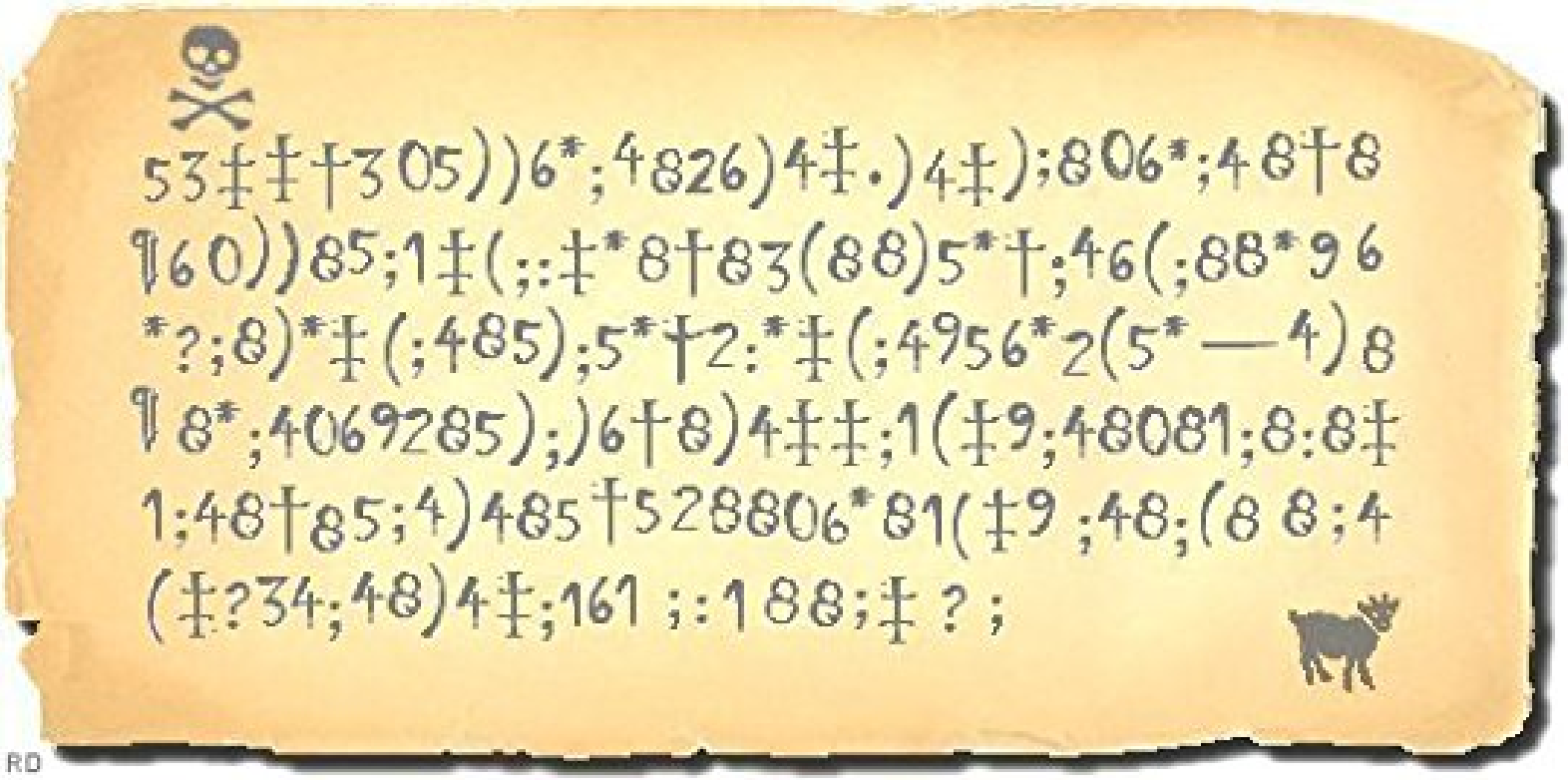
Перевод

Пришёл, увидел, победил

Расшифровка

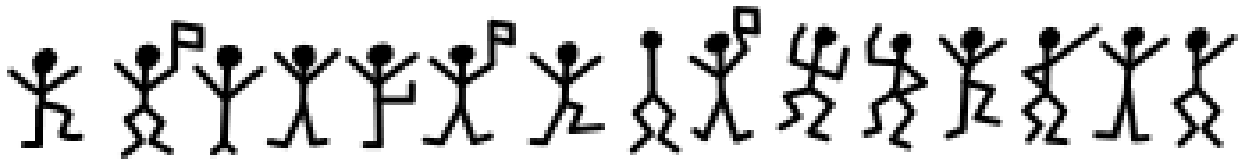
Veni, vidi, vici

Шифры заменой в литературе



Зашифрованное сообщение из рассказа Эдгара Аллана По “Золотой жук”

Шифры заменой в литературе



Зашифрованное сообщение из рассказа Артура Конан Дойля “Пляшущие человечки”

Шифры заменой

Буквы — числа

Каждая буква алфавита заменяется на число

Пример

Заменим букву А на букву 1, букву Б — на 2, букву В — на 3 и так далее. Букву Я заменим на 33.

Задача

Расшифруйте 22122111121 (должно получиться осмысленное слово)

Шифры заменой

Буквы — числа

Каждая буква алфавита заменяется на число

Пример

Заменим букву А на букву 1, букву Б — на 2, букву В — на 3 и так далее. Букву Я заменим на 33.

Задача

Расшифруйте 22122111121 (должно получиться осмысленное слово)

Шифры заменой

Буквы — числа

Каждая буква алфавита заменяется на число

Пример

Заменим букву А на букву 1, букву Б — на 2, букву В — на 3 и так далее. Букву Я заменим на 33.

Задача

Расшифруйте 222122111121 (должно получиться осмысленное слово)

Как разгадать шифр заменой

Частотный анализ

ОЕАИНТ СРВЛКМ

Английский алфавит

ETAOIN SHRDLU

Примѣръ статистическаго изслѣдованія надъ текстомъ „Евгенія Онѣгина“ иллюстрирующій связь испытаній въ цѣпь.

А. А. Марковъ.

(Доложено въ засѣданіи Физико-Математическаго Отдѣленія 23 января 1913 г.).

Наше изслѣдованіе относится къ послѣдовательности 20 000 русскихъ буквъ, не считая ъ и ь, въ романѣ А. С. Пушкина «Евгеній Онѣгинъ», *которая заполняетъ всю первую главу и шестьнадцать строфъ второй.*

Эта послѣдовательность доставляетъ намъ 20 000 связанныхъ испытаній, каждое изъ которыхъ даетъ гласную или согласную букву.

Соотвѣтственно этому мы допускаемъ существованіе неизвѣстной постоянной вѣроятности p буквѣ быть гласной и приближенную величину числа p вщемъ изъ наблюденій, считая число появившихся гласныхъ и согласныхъ буквъ. Кромѣ числа p мы найдемъ, также изъ наблюденій, приближенныя величины двухъ чиселъ p_1 и p_0 и четырехъ чиселъ $p_{1,1}$, $p_{1,0}$, $p_{0,1}$, $p_{0,0}$, представляющихъ такія вѣроятности: p_1 — гласной слѣдовать за гласной, p_0 — гласной слѣдовать за согласной, $p_{1,1}$ — гласной слѣдовать за двумя гласными, $p_{1,0}$ — гласной слѣдовать за согласной, которой предшествуетъ гласная, $p_{0,1}$ — гласной слѣдовать за гласной, которой предшествуетъ согласная и, наконецъ, $p_{0,0}$ — гласной слѣдовать за двумя согласными.

Как разгадать шифр заменой

Частотный анализ

ОЕАИНТ СРВЛКМ

Английский алфавит

ETAOIN SHRDLU

Примѣръ статистическаго изслѣдованія надъ текстомъ „Евгенія Онѣгина“ иллюстрирующій связь испытаній въ цѣпь.

А. А. Марковъ.

(Доложено въ засѣданіи Физико-Математическаго Отдѣленія 23 января 1913 г.).

Наше изслѣдованіе относится къ послѣдовательности 20 000 русскихъ буквъ, не считая ъ и ь, въ романѣ А. С. Пушкина «Евгеній Онѣгинъ», *которая заполняетъ всю первую главу и шестьнадцать строфъ второй.*

Эта послѣдовательность доставляетъ намъ 20 000 связанныхъ испытаній, каждое изъ которыхъ даетъ гласную или согласную букву.

Соотвѣтственно этому мы допускаемъ существованіе неизвѣстной постоянной вѣроятности p буквѣ быть гласной и приближенную величину числа p вщемъ изъ наблюденій, считая число появившихся гласныхъ и согласныхъ буквъ. Кромѣ числа p мы найдемъ, также изъ наблюденій, приближенныя величины двухъ чиселъ p_1 и p_0 и четырехъ чиселъ $p_{1,1}$, $p_{1,0}$, $p_{0,1}$, $p_{0,0}$, представляющихъ такія вѣроятности: p_1 — гласной слѣдовать за гласной, p_0 — гласной слѣдовать за согласной, $p_{1,1}$ — гласной слѣдовать за двумя гласными, $p_{1,0}$ — гласной слѣдовать за согласной, которой предшествуетъ гласная, $p_{0,1}$ — гласной слѣдовать за гласной, которой предшествуетъ согласная и, наконецъ, $p_{0,0}$ — гласной слѣдовать за двумя согласными.

Как разгадать шифр заменой

Частотный анализ

ОЕАИНТ СРВЛКМ

Английский алфавит

ETAOIN SHRDLU

Примѣръ статистическаго изслѣдованія надъ текстомъ „Евгенія Онѣгина“ иллюстрирующій связь испытаній въ цѣпь.

А. А. Марковъ.

(Доложено въ засѣданіи Физико-Математическаго Отдѣленія 23 января 1913 г.).

Наше изслѣдованіе относится къ послѣдовательности 20 000 русскихъ буквъ, не считая ъ и ь, въ романѣ А. С. Пушкина «Евгеній Онѣгинъ», *которая заполняетъ всю первую главу и шестьнадцать строфъ второй.*

Эта послѣдовательность доставляетъ намъ 20 000 связанныхъ испытаній, каждое изъ которыхъ даетъ гласную или согласную букву.

Соотвѣтственно этому мы допускаемъ существованіе неизвѣстной постоянной вѣроятности p буквѣ быть гласной и приближенную величину числа p вщемъ изъ наблюденій, считая число появившихся гласныхъ и согласныхъ буквъ. Кромѣ числа p мы найдемъ, также изъ наблюденій, приближенныя величины двухъ чиселъ p_1 и p_0 и четырехъ чиселъ $p_{1,1}$, $p_{1,0}$, $p_{0,1}$, $p_{0,0}$, представляющихъ такія вѣроятности: p_1 — гласной слѣдовать за гласной, p_0 — гласной слѣдовать за согласной, $p_{1,1}$ — гласной слѣдовать за двумя гласными, $p_{1,0}$ — гласной слѣдовать за согласной, которой предшествуетъ гласная, $p_{0,1}$ — гласной слѣдовать за гласной, которой предшествуетъ согласная и, наконецъ, $p_{0,0}$ — гласной слѣдовать за двумя согласными.

Как разгадать шифр заменой

Частотный анализ

ОЕАИНТ СРВЛКМ

Английский алфавит

ETAOIN SHRDLU

Примѣръ статистическаго изслѣдованія надъ текстомъ „Евгенія Онѣгина“ иллюстрирующій связь испытаній въ цѣпь.

А. А. Марковъ.

(Доложено въ засѣданіи Физико-Математическаго Отдѣленія 23 января 1913 г.).

Наше изслѣдованіе относится къ послѣдовательности 20 000 русскихъ буквъ, не считая ъ и ь, въ романѣ А. С. Пушкина «Евгеній Онѣгинъ», *которая заполняетъ всю первую главу и шестьнадцать строфъ второй.*

Эта послѣдовательность доставляетъ намъ 20 000 связанныхъ испытаній, каждое изъ которыхъ даетъ гласную или согласную букву.

Соотвѣтственно этому мы допускаемъ существованіе неизвѣстной постоянной вѣроятности p буквѣ быть гласной и приближенную величину числа p вщемъ изъ наблюденій, считая число появившихся гласныхъ и согласныхъ буквъ. Кромѣ числа p мы найдемъ, также изъ наблюденій, приближенныя величины двухъ чиселъ p_1 и p_0 и четырехъ чиселъ $p_{1,1}$, $p_{1,0}$, $p_{0,1}$, $p_{0,0}$, представляющихъ такія вѣроятности: p_1 — гласной слѣдовать за гласной, p_0 — гласной слѣдовать за согласной, $p_{1,1}$ — гласной слѣдовать за двумя гласными, $p_{1,0}$ — гласной слѣдовать за согласной, которой предшествуетъ гласная, $p_{0,1}$ — гласной слѣдовать за гласной, которой предшествуетъ согласная и, наконецъ, $p_{0,0}$ — гласной слѣдовать за двумя согласными.

Как разгадать шифр заменой

Частотный анализ

ОЕАИНТ СРВЛКМ

Английский алфавит

ETAOIN SHRDLU

Примѣръ статистическаго изслѣдованія надъ текстомъ „Евгенія Онѣгина“ иллюстрирующій связь испытаній въ цѣпь.

А. А. Марковъ.

(Доложено въ засѣданіи Физико-Математическаго Отдѣленія 23 января 1913 г.).

Наше изслѣдованіе относится къ послѣдовательности 20 000 русскихъ буквъ, не считая ъ и ь, въ романѣ А. С. Пушкина «Евгеній Онѣгинъ», *которая заполняетъ всю первую главу и шестьнадцать строфъ второй.*

Эта послѣдовательность доставляетъ намъ 20 000 связанныхъ испытаній, каждое изъ которыхъ даетъ гласную или согласную букву.

Соотвѣтственно этому мы допускаемъ существованіе неизвѣстной постоянной вѣроятности p буквѣ быть гласной и приближенную величину числа p вщемъ изъ наблюденій, считая число появившихся гласныхъ и согласныхъ буквъ. Кромѣ числа p мы найдемъ, также изъ наблюденій, приближенныя величины двухъ чиселъ p_1 и p_0 и четырехъ чиселъ $p_{1,1}$, $p_{1,0}$, $p_{0,1}$, $p_{0,0}$, представляющихъ такія вѣроятности: p_1 — гласной слѣдовать за гласной, p_0 — гласной слѣдовать за согласной, $p_{1,1}$ — гласной слѣдовать за двумя гласными, $p_{1,0}$ — гласной слѣдовать за согласной, которой предшествуетъ гласная, $p_{0,1}$ — гласной слѣдовать за гласной, которой предшествуетъ согласная и, наконецъ, $p_{0,0}$ — гласной слѣдовать за двумя согласными.

Как разгадать шифр заменой

Зашифрована детская песенка

Фвжгмяф, Фвжгмяф, дгюшъб ягдфжр яфежгмяз,
Фвжгмяф, Фвжгмяф, дгюшъб ягдфжр яфежгмяз!
Жэаэ-жэаэ жефаэ-цфаэ.
Сжг бп вщ дегйгшэаэ, сжг вфб вщ ьфшфцфаэ.
Жэаэ-жэаэ, жефаэ-цфаэ.
Сжг бп вщ дегйгшэаэ, сжг вфб вщ ьфшфцфаэ.
Дф-ефб-дфб-дфб, Дф-ефб-дфб-дфб.

Как разгадать шифр заменой

Какая буква встречается чаще всего?

Фвжгмяф, Фвжгмяф, дгюшъб ягдфжр яфежгмяз,
Фвжгмяф, Фвжгмяф, дгюшъб ягдфжр яфежгмяз!
Жэаэ-жэаэ жефаэ-цфаэ.
Сжг бп вщ дегйгшэаэ, сжг вфб вщ ьфшфцфаэ.
Жэаэ-жэаэ, жефаэ-цфаэ.
Сжг бп вщ дегйгшэаэ, сжг вфб вщ ьфшфцфаэ.
Дф-ефб-дфб-дфб, Дф-ефб-дфб-дфб.

Как разгадать шифр заменой

Попробуем заменить Ф на О, А, Е или И

Авжгмяа, Авжгмяа, дгюшъб ягдажр яаежгмяз,
Авжгмяа, Авжгмяа, дгюшъб ягдажр яаежгмяз!
Жэаэ-жэаэ жеааэ-цааэ.
Сжг бп вщ дегйгшэаэ, сжг ваб вщ ьашацааэ.
Жэаэ-жэаэ, жеааэ-цааэ.
Сжг бп вщ дегйгшэаэ, сжг ваб вщ ьашацааэ.
Да-еаб-даб-даб, Да-еаб-даб-даб.

Как разгадать шифр заменой

Какая буква — вторая по частоте?

Авжгмяа, Авжгмяа, дгюшъб ягдажр яаежгмяз,
Авжгмяа, Авжгмяа, дгюшъб ягдажр яаежгмяз!
Жэаэ-жэаэ жеааэ-цааэ.
Сжг бп вщ дегйгшэаэ, сжг ваб вщ ьашацааэ.
Жэаэ-жэаэ, жеааэ-цааэ.
Сжг бп вщ дегйгшэаэ, сжг ваб вщ ьашацааэ.
Да-еаб-даб-даб, Да-еаб-даб-даб.

Как разгадать шифр заменой

Заменим Г на О

Авжомяа, Авжомяа, доюшъб яодажр яаежомяз,
Авжомяа, Авжомяа, доюшъб яодажр яаежомяз!
Жэаэ-жэаэ жеааэ-цааэ.
Сжо бп вщ деойошэаэ, сжо ваб вщ ьашацааэ.
Жэаэ-жэаэ, жеааэ-цааэ.
Сжо бп вщ деойошэаэ, сжо ваб вщ ьашацааэ.
Да-еаб-даб-даб, Да-еаб-даб-даб.

Как разгадать шифр заменой

Настолько же часто встречается Ж

Авжомяа, Авжомяа, доюшъб яодажр яаежомяз,
Авжомяа, Авжомяа, доюшъб яодажр яаежомяз!
Жэаэ-жэаэ жеааэ-цааэ.
Сжо бп вщ деойошэаэ, сжо ваб вщ ьашацааэ.
Жэаэ-жэаэ, жеааэ-цааэ.
Сжо бп вщ деойошэаэ, сжо ваб вщ ьашацааэ.
Да-еаб-даб-даб, Да-еаб-даб-даб.

Как разгадать шифр заменой

Попробуем заменить Ж на Н, Т, Р или С

Автомяа, Автомяа, доюшъб яодатр яаетомяз,
Автомяа, Автомяа, доюшъб яодатр яаетомяз!
Тэаэ-тэаэ теааэ-цааэ.
Сто бп вщ деойошэаэ, сто ваб вщ ьашацааэ.
Тэаэ-тэаэ, теааэ-цааэ.
Сто бп вщ деойошэаэ, сто ваб вщ ьашацааэ.
Да-еаб-даб-даб, Да-еаб-даб-даб.

Как разгадать шифр заменой

И настолько же часто встречается Э

Автомяа, Автомяа, доюшъб яодатр яаетомяз,
Автомяа, Автомяа, доюшъб яодатр яаетомяз!
Тэаэ-тэаэ теааэ-цааэ.
Сто бп вщ деойошэаэ, сто ваб вщ ьашацааэ.
Тэаэ-тэаэ, теааэ-цааэ.
Сто бп вщ деойошэаэ, сто ваб вщ ьашацааэ.
Да-еаб-даб-даб, Да-еаб-даб-даб.

Как разгадать шифр заменой

Попробуем заменить Э на И

Автомяа, Автомяа, доюшъб яодатр яаетомяз,
Автомяа, Автомяа, доюшъб яодатр яаетомяз!
Тиаи-тиаи теааи-цааи.
Сто бп вщ деойошиаи, сто ваб вщ ьашацааи.
Тиаи-тиаи, теааи-цааи.
Сто бп вщ деойошиаи, сто ваб вщ ьашацааи.
Да-еаб-даб-даб, Да-еаб-даб-даб.

Как разгадать шифр заменой

Первое слово — это явно имя. Какое?

Автомяа, Автомяа, доюшъб яодатр яаетомяз,
Автомяа, Автомяа, доюшъб яодатр яаетомяз!
Тиаи-тиаи теааи-цааи.
Сто бп вщ деойошиаи, сто ваб вщ ьашацааи.
Тиаи-тиаи, теааи-цааи.
Сто бп вщ деойошиаи, сто ваб вщ ьашацааи.
Да-еаб-даб-даб, Да-еаб-даб-даб.

Отгадка

Антошка, Антошка, пойдём копать картошку,
Антошка, Антошка, пойдём копать картошку!
Тили-тили трали-вали.
Это мы не проходили, это нам не задавали.
Тили-тили, трали-вали.
Это мы не проходили, это нам не задавали.
Па-рам-пам-пам,
Па-рам-пам-пам

Шифр-решётка

Т	У	Р	С	Ю	Г
И	Т	Н	Ь	Ш	А
А	З	А	Я	Р	Д
Е	В	А	Г	А	Н
П	А	Ш	А	А	Д
К	И	Г	О	А	Т

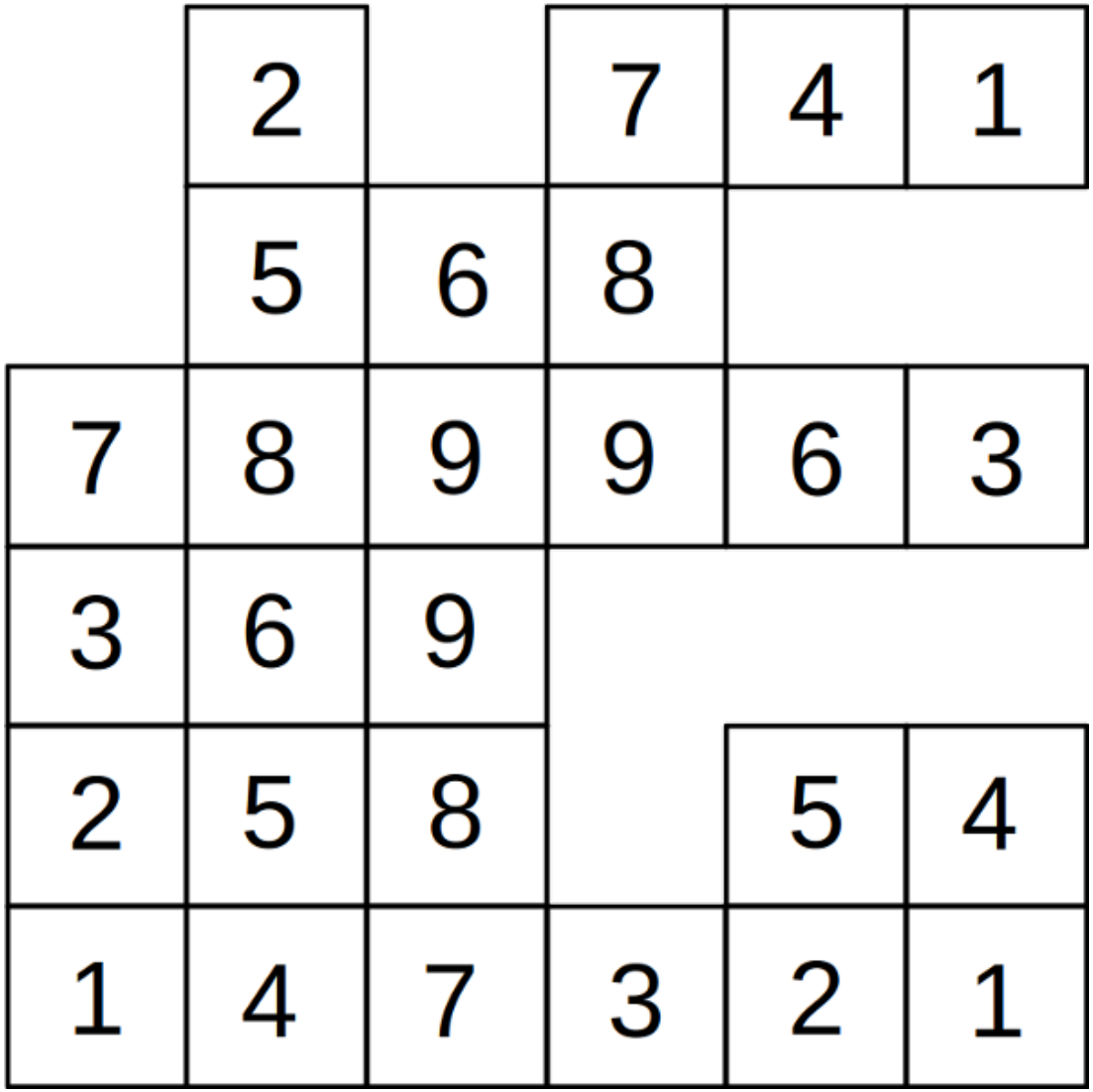
Другая идея

Чтобы шифр было сложнее разгадать, нужно ПЕРЕСТАВЛЯТЬ буквы.

Шифр-решётка

Ключ

Чтобы разгадать сообщение нужен КЛЮЧ — секретный трафарет.



Шифр-решётка

Т	2	**Р**	7	4	1
И	5	6	8	**Ш**	**А**
7	8	9	9	6	3
3	6	9	**Г**	**А**	**Н**
2	5	8	**А**	5	4
1	4	7	3	2	1

Расшифровка — первый шаг

Прикладываем трафарет к сообщению и читаем слева направо и сверху вниз:

ТРИШАГАНА

Расставляем пробелы

ТРИ ШАГА НА

Шифр-решётка

Расшифровка — первый шаг

Прикладываем трафарет к сообщению и читаем слева направо и сверху вниз:
ТРИШАГАНА

Расставляем пробелы
ТРИ ШАГА НА

Т	2	**Р**	7	4	1
И	5	6	8	**Ш**	**А**
7	8	9	9	6	3
3	6	9	**Г**	**А**	**Н**
2	5	8	**А**	5	4
1	4	7	3	2	1

Шифр-решётка

Расшифровка — первый шаг

Прикладываем трафарет к сообщению и читаем слева направо и сверху вниз:

ТРИШАГАНА

Расставляем пробелы

ТРИ ШАГА НА

Т	2	**Р**	7	4	1
И	5	6	8	**Ш**	**А**
7	8	9	9	6	3
3	6	9	**Г**	**А**	**Н**
2	5	8	**А**	5	4
1	4	7	3	2	1

Шифр-решётка

Расшифровка — первый шаг

Прикладываем трафарет к сообщению и читаем слева направо и сверху вниз:

ТРИШАГАНА

Расставляем пробелы

ТРИ ШАГА НА

Т	2	**Р**	7	4	1
И	5	6	8	**Ш**	**А**
7	8	9	9	6	3
3	6	9	**Г**	**А**	**Н**
2	5	8	**А**	5	4
1	4	7	3	2	1

Шифр-решётка

Расшифровка — первый шаг

Прикладываем трафарет к сообщению и читаем слева направо и сверху вниз:

ТРИШАГАНА

Расставляем пробелы

ТРИ ШАГА НА

Т	2	**Р**	7	4	1
И	5	6	8	**Ш**	**А**
7	8	9	9	6	3
3	6	9	**Г**	**А**	**Н**
2	5	8	**А**	5	4
1	4	7	3	2	1

Шифр-решётка

1	2	3	7	Ю	Г
4	5	6	8	5	2
7	8	9	9	6	Д
3	В	А	9	8	7
2	5	Ш	6	А	4
1	4	Г	3	А	1

Расшифровка — второй шаг.

Поворачиваем трафарет на 90 градусов.

ЮГДВАШАГА

Расставляем пробелы

ЮГ ДВА ШАГА

Шифр-решётка

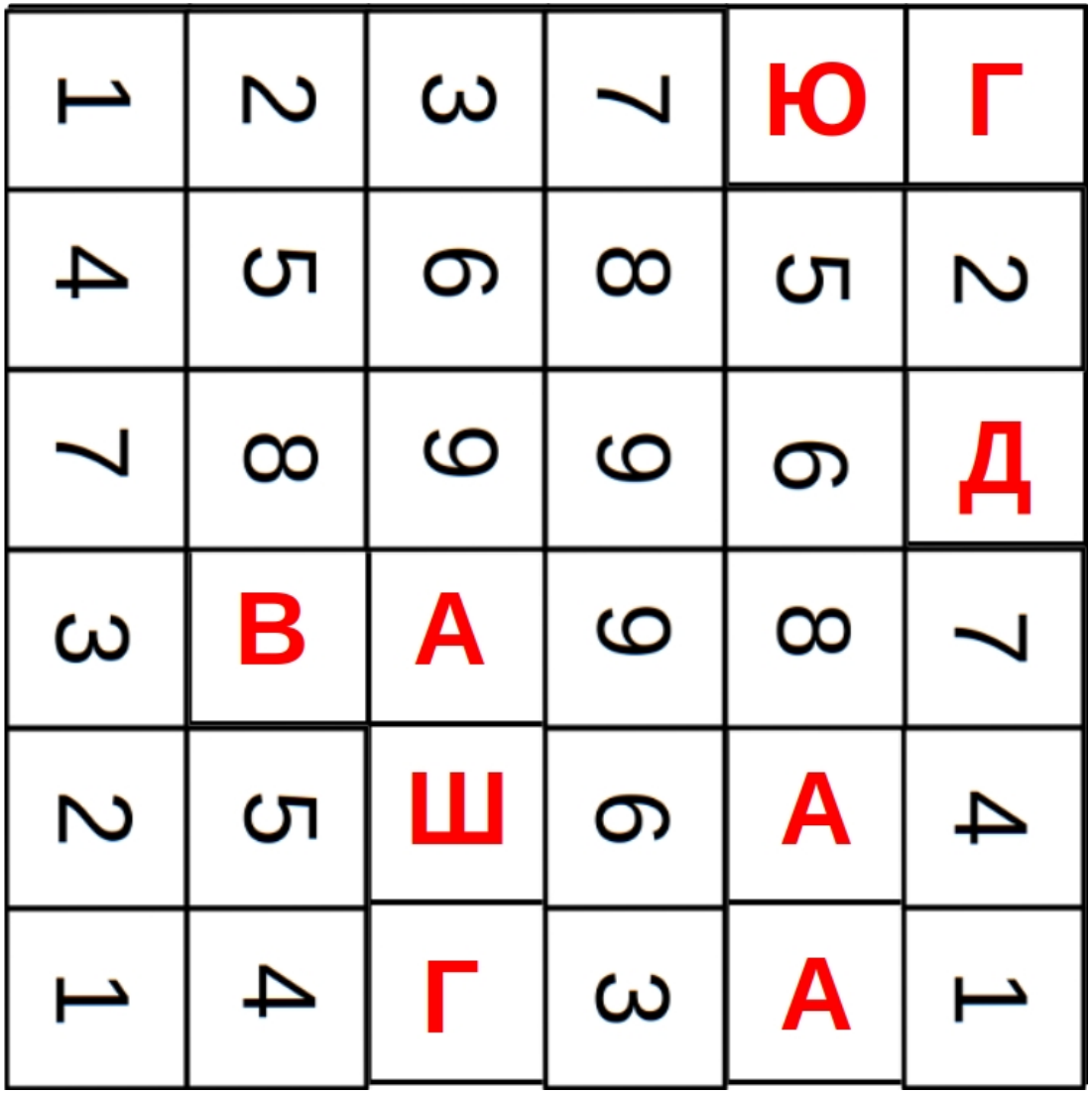
Расшифровка — второй шаг

Поворачиваем трафарет на 90 градусов.

ЮГДВАШАГА

Расставляем пробелы

ЮГ ДВА ШАГА



Шифр-решётка

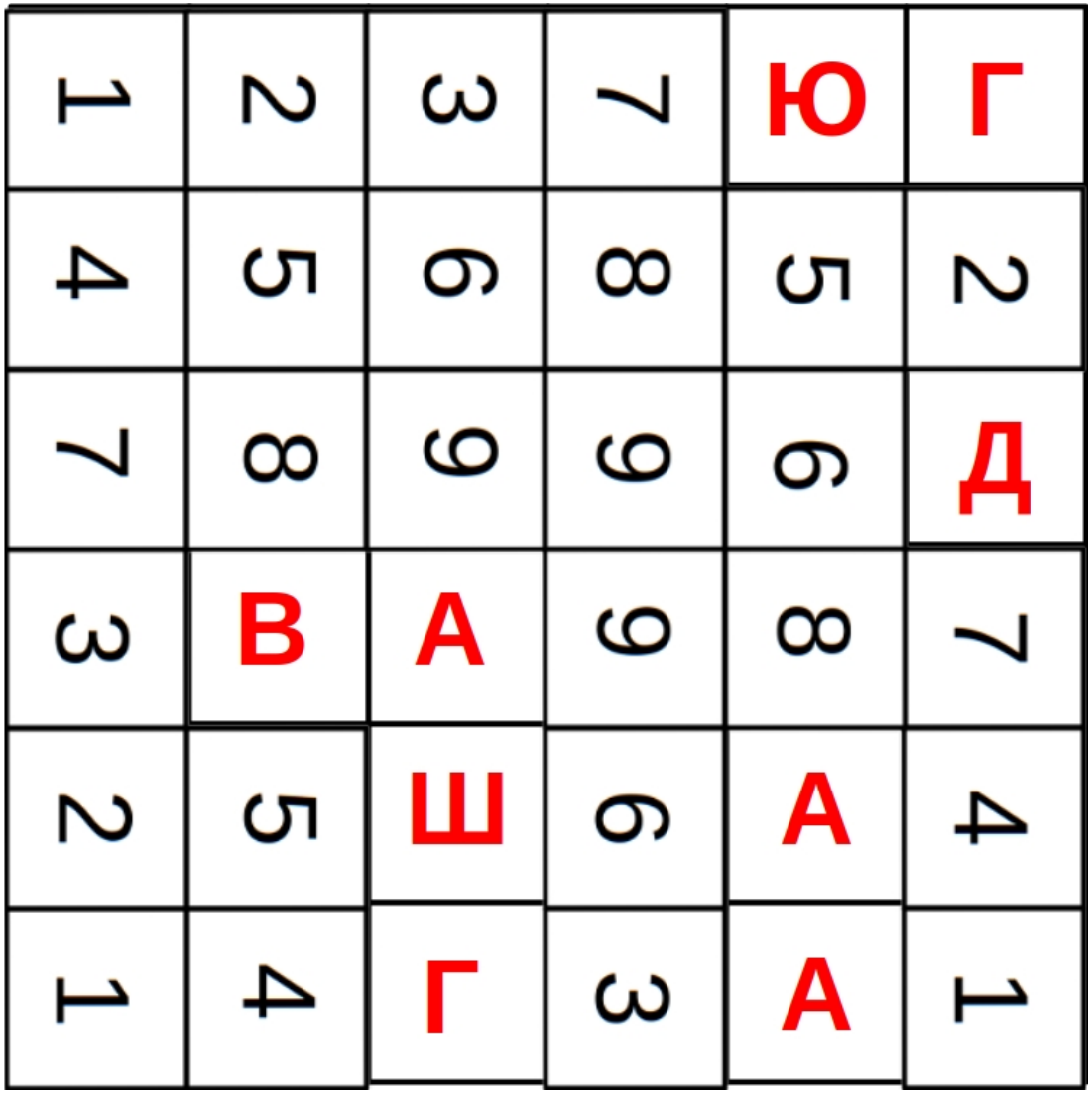
Расшифровка — второй шаг

Поворачиваем трафарет на 90 градусов.

ЮГДВАШАГА

Расставляем пробелы

ЮГ ДВА ШАГА



Шифр-решётка

Расшифровка — второй шаг

Поворачиваем трафарет на 90 градусов.

ЮГДВАШАГА

Расставляем пробелы

ЮГ ДВА ШАГА

1	2	3	7	Ю	Г
4	5	6	8	5	2
7	8	9	9	6	Д
3	В	А	9	8	7
2	5	Ш	6	А	4
1	4	Г	3	А	1

Шифр-решётка

Расшифровка — второй шаг

Поворачиваем трафарет на 90 градусов.

ЮГДВАШАГА

Расставляем пробелы

ЮГ ДВА ШАГА

1	2	3	7	Ю	Г
4	5	6	8	5	2
7	8	9	9	6	Д
3	В	А	9	8	7
2	5	Ш	6	А	4
1	4	Г	3	А	1

Шифр-решётка

Расшифровка — третий шаг.

Второй раз поворачиваем трафарет на 90 градусов.

НАЗАПАДОТ

Расставляем пробелы

НА ЗАПАД ОТ

Шифр-решётка

Расшифровка — третий шаг

Второй раз поворачиваем трафарет на 90 градусов.

НАЗАПАДОТ

Расставляем пробелы

НА ЗАПАД ОТ

Шифр-решётка

Расшифровка — третий шаг

Второй раз поворачиваем трафарет на 90 градусов.

НАЗАПАДОТ

Расставляем пробелы

НА ЗАПАД ОТ

Шифр-решётка

Расшифровка — третий шаг

Второй раз поворачиваем трафарет на 90 градусов.

НАЗАПАДОТ

Расставляем пробелы

НА ЗАПАД ОТ

Шифр-решётка

Расшифровка — третий шаг

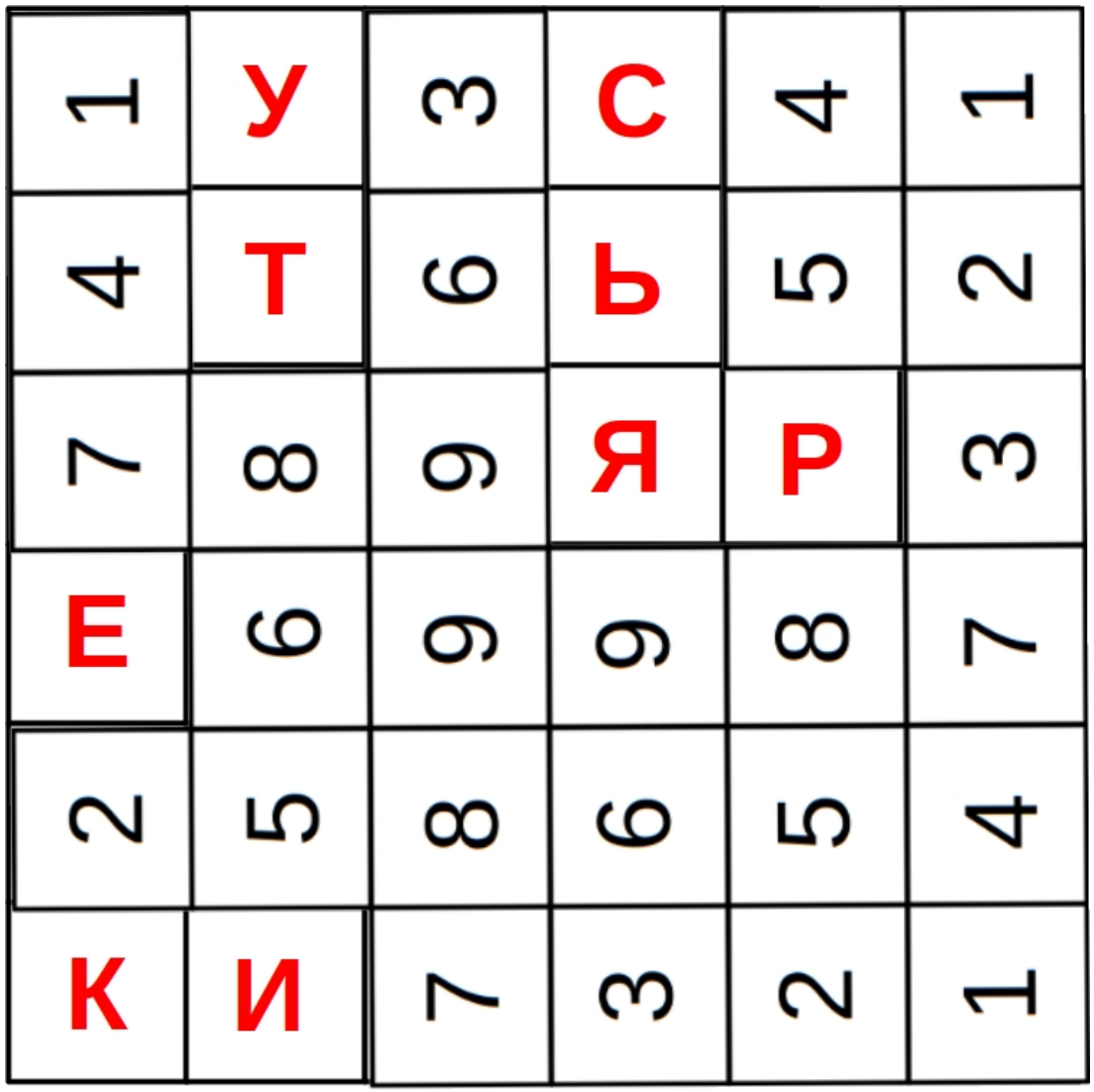
Второй раз поворачиваем трафарет на 90 градусов.

НАЗАПАДОТ

Расставляем пробелы

НА ЗАПАД ОТ

Шифр-решётка



Расшифровка — четвёртый шаг

Третий раз поворачиваем трафарет на 90 градусов.

ОТУСТЬЯРЕКИ

Расставляем пробелы

ОТ УСТЬЯ РЕКИ

Шифр-решётка

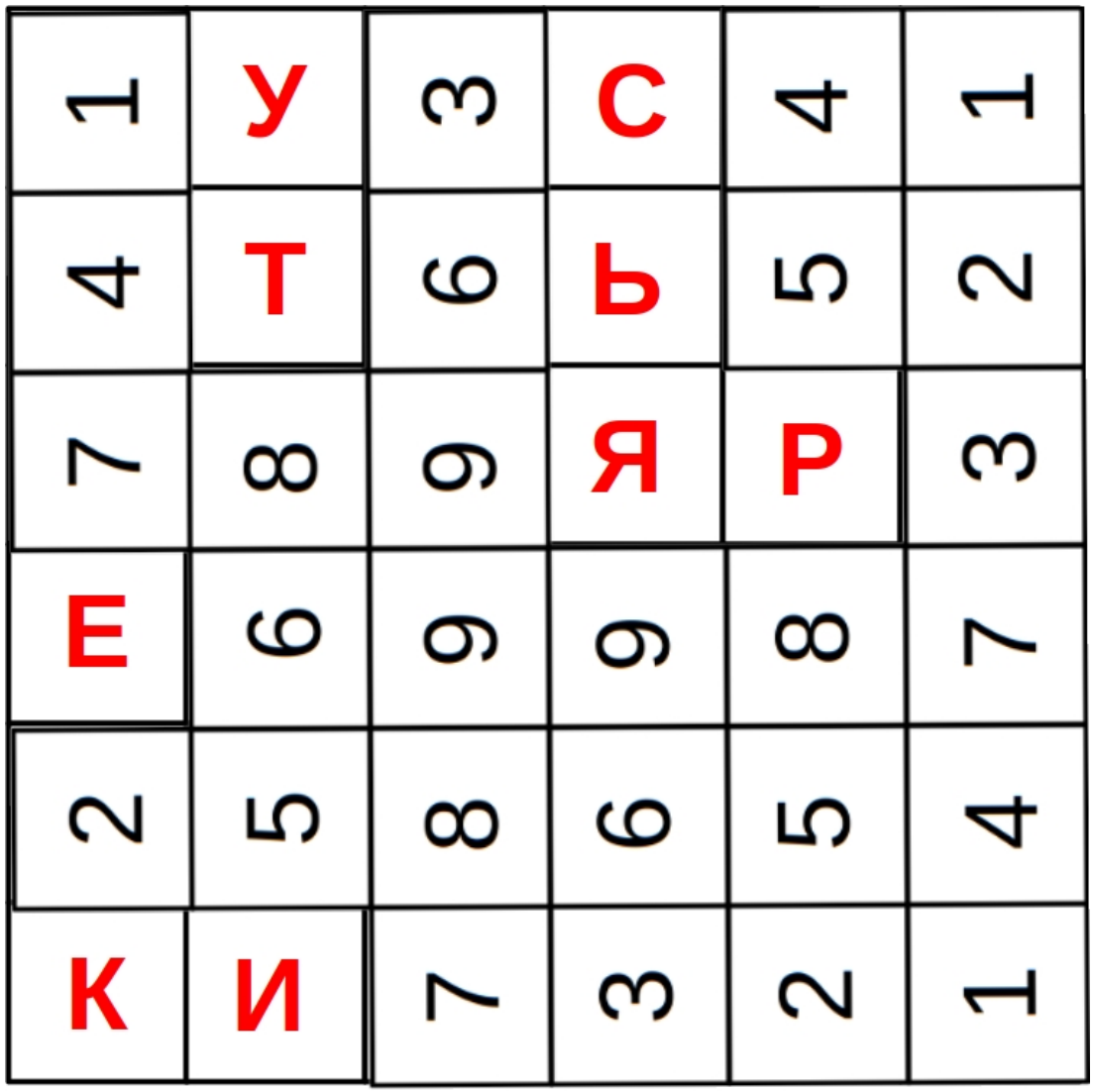
Расшифровка — четвёртый шаг

Третий раз поворачиваем трафарет на 90 градусов.

ОТУСТЬЯРЕКИ

Расставляем пробелы

ОТ УСТЬЯ РЕКИ

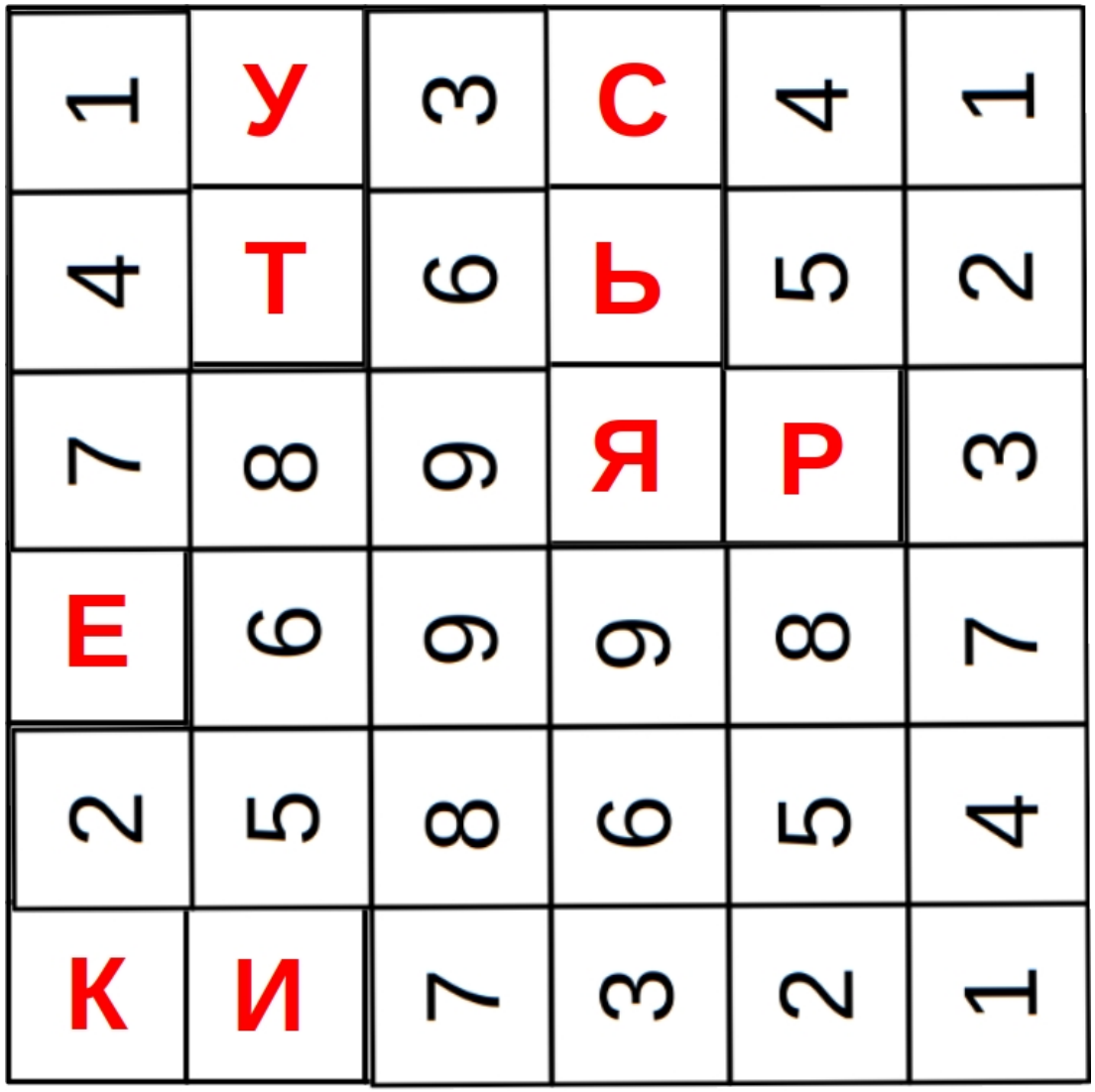


Шифр-решётка

Расшифровка — четвёртый шаг

Третий раз поворачиваем трафарет на 90 градусов.
ОТУСТЬЯРЕКИ

Расставляем пробелы
ОТ УСТЬЯ РЕКИ



Шифр-решётка

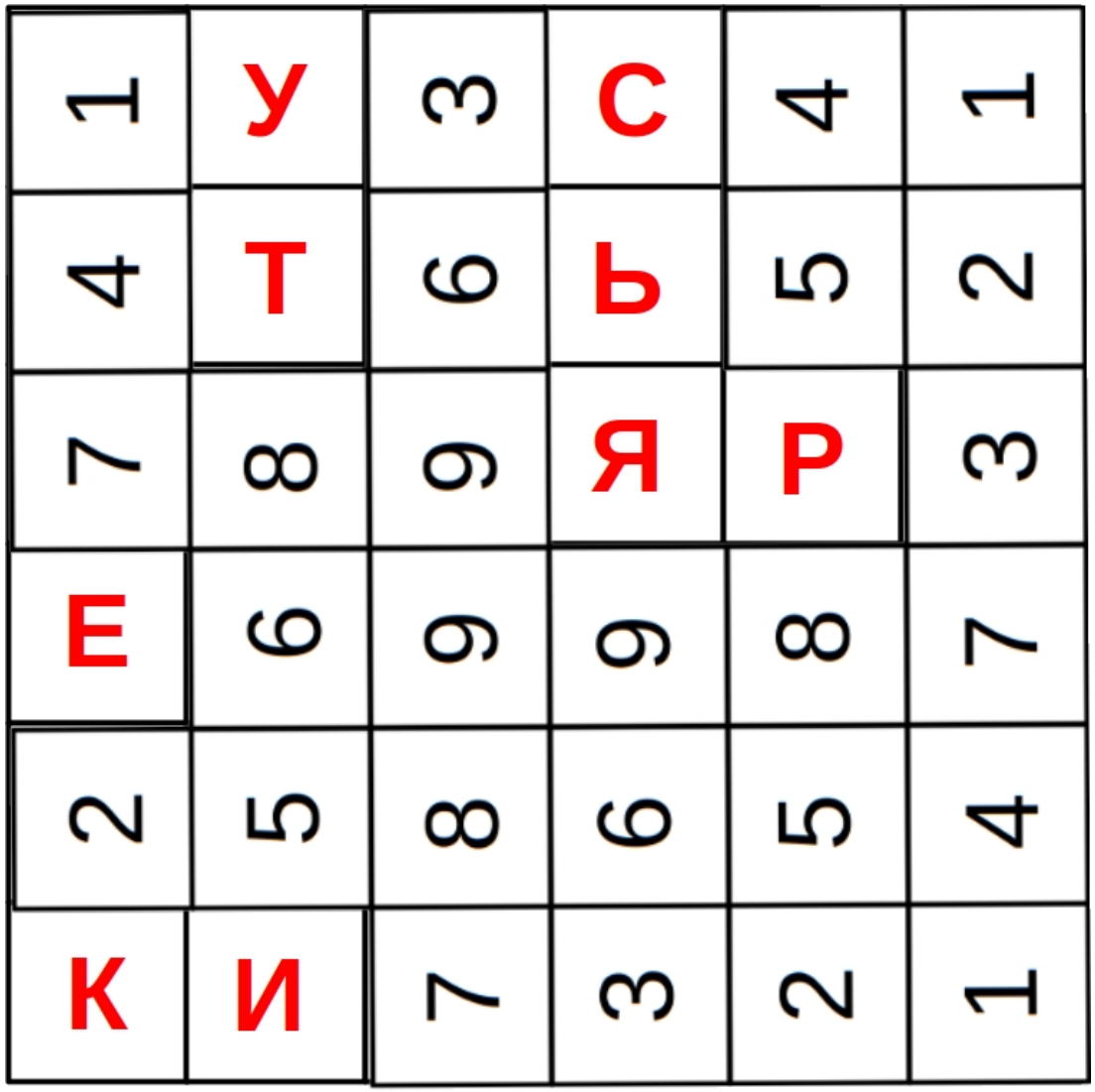
Расшифровка — четвёртый шаг

Третий раз поворачиваем трафарет на 90 градусов.

ОТУСТЬЯРЕКИ

Расставляем пробелы

ОТ УСТЬЯ РЕКИ



Шифр-решётка

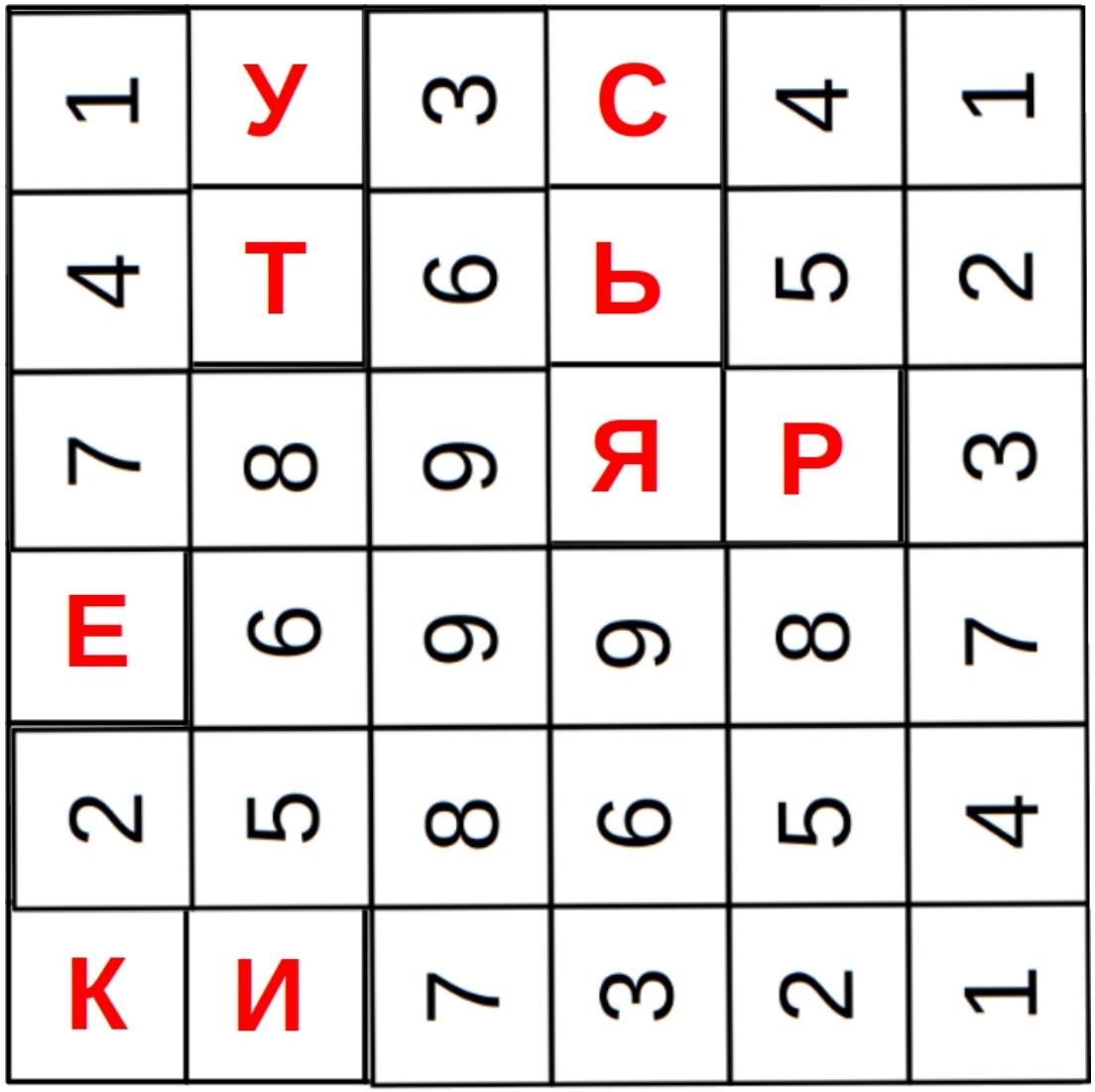
Расшифровка — четвёртый шаг

Третий раз поворачиваем трафарет на 90 градусов.

ОТУСТЬЯРЕКИ

Расставляем пробелы

ОТ УСТЬЯ РЕКИ



Шифр-решётка

Т	У	Р	С	Ю	Г
И	Т	Н	Ь	Ш	А
А	З	А	Я	Р	Д
Е	В	А	Г	А	Н
П	А	Ш	А	А	Д
К	И	Г	О	А	Т

Отгадка

ТРИ ШАГА НА ЗАПАД
ДВА ШАГА НА ЮГ ОТ
УСТЬЯ РЕКИ

Шифр-решётка

Т	У	Р	С	Ю	Г
И	Т	Н	Ь	Ш	А
А	З	А	Я	Р	Д
Е	В	А	Г	А	Н
П	А	Ш	А	А	Д
К	И	Г	О	А	Т

Отгадка

ТРИ ШАГА НА ЗАПАД
ДВА ШАГА НА ЮГ ОТ
УСТЬЯ РЕКИ

Шифр-решётка

Отгадка

ТРИ ШАГА НА ЗАПАД
ДВА ШАГА НА ЮГ ОТ
УСТЬЯ РЕКИ

Т	У	Р	С	Ю	Г
И	Т	Н	Ь	Ш	А
А	З	А	Я	Р	Д
Е	В	А	Г	А	Н
П	А	Ш	А	А	Д
К	И	Г	О	А	Т

Шифр-решётка

Отгадка

ТРИ ШАГА НА ЗАПАД
ДВА ШАГА НА ЮГ ОТ
УСТЬЯ РЕКИ

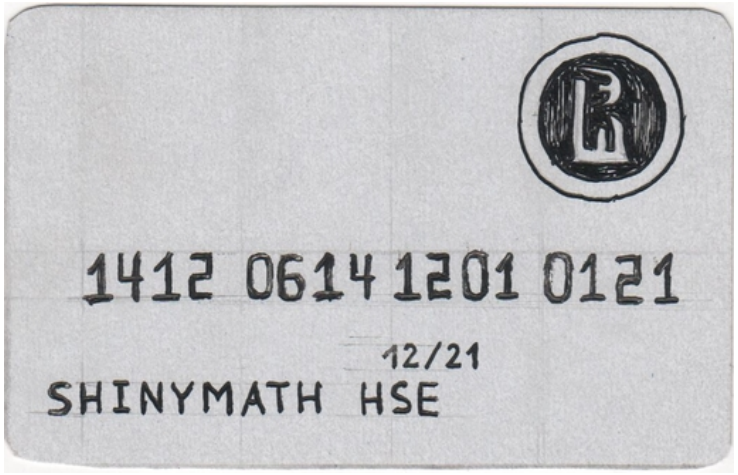
Т	У	Р	С	Ю	Г
И	Т	Н	Ь	Ш	А
А	З	А	Я	Р	Д
Е	В	А	Г	А	Н
П	А	Ш	А	А	Д
К	И	Г	О	А	Т

Где зарыт клад

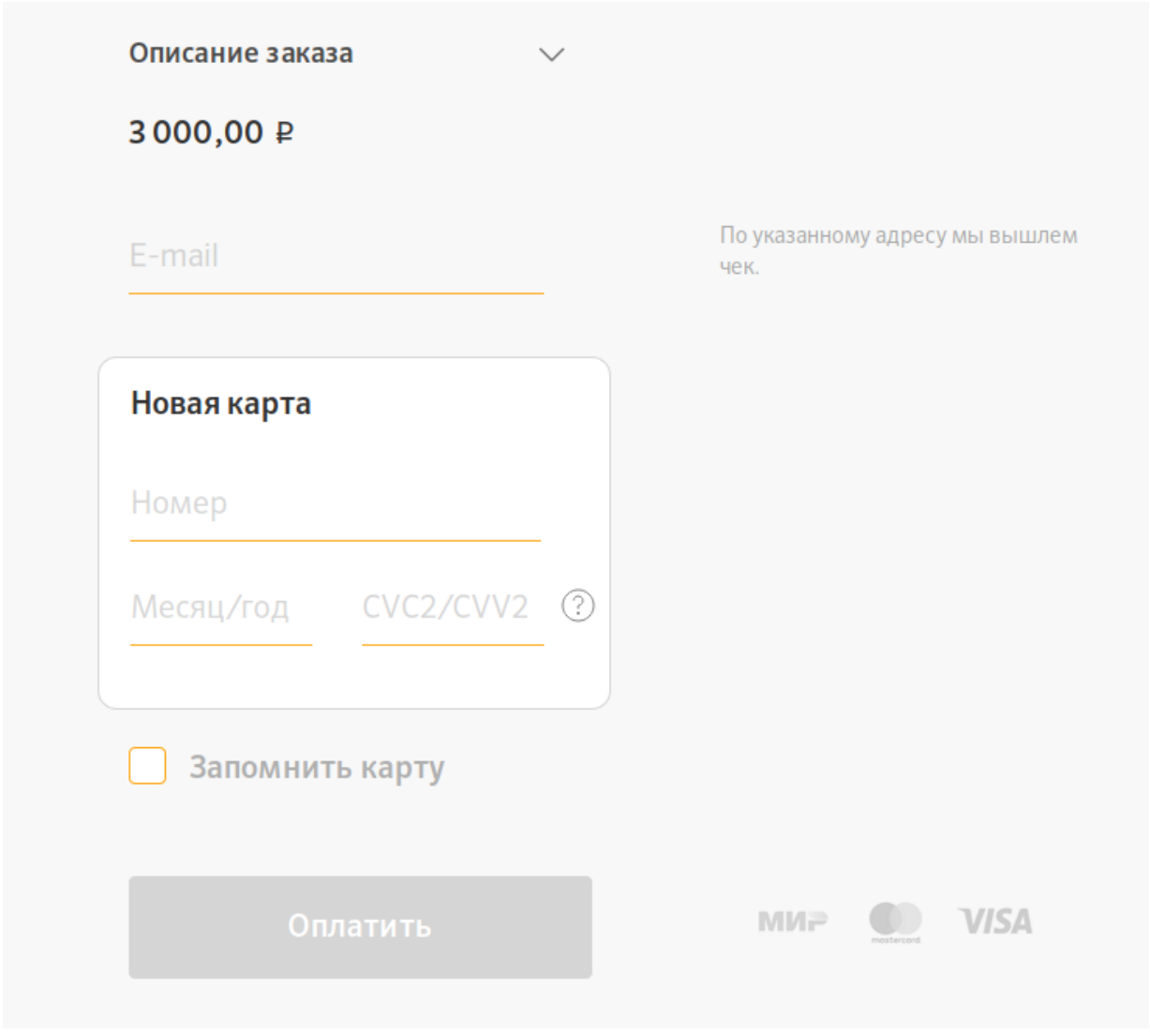
Практическая задача

Покупки онлайн

Как зашифровать данные кредитной карты?

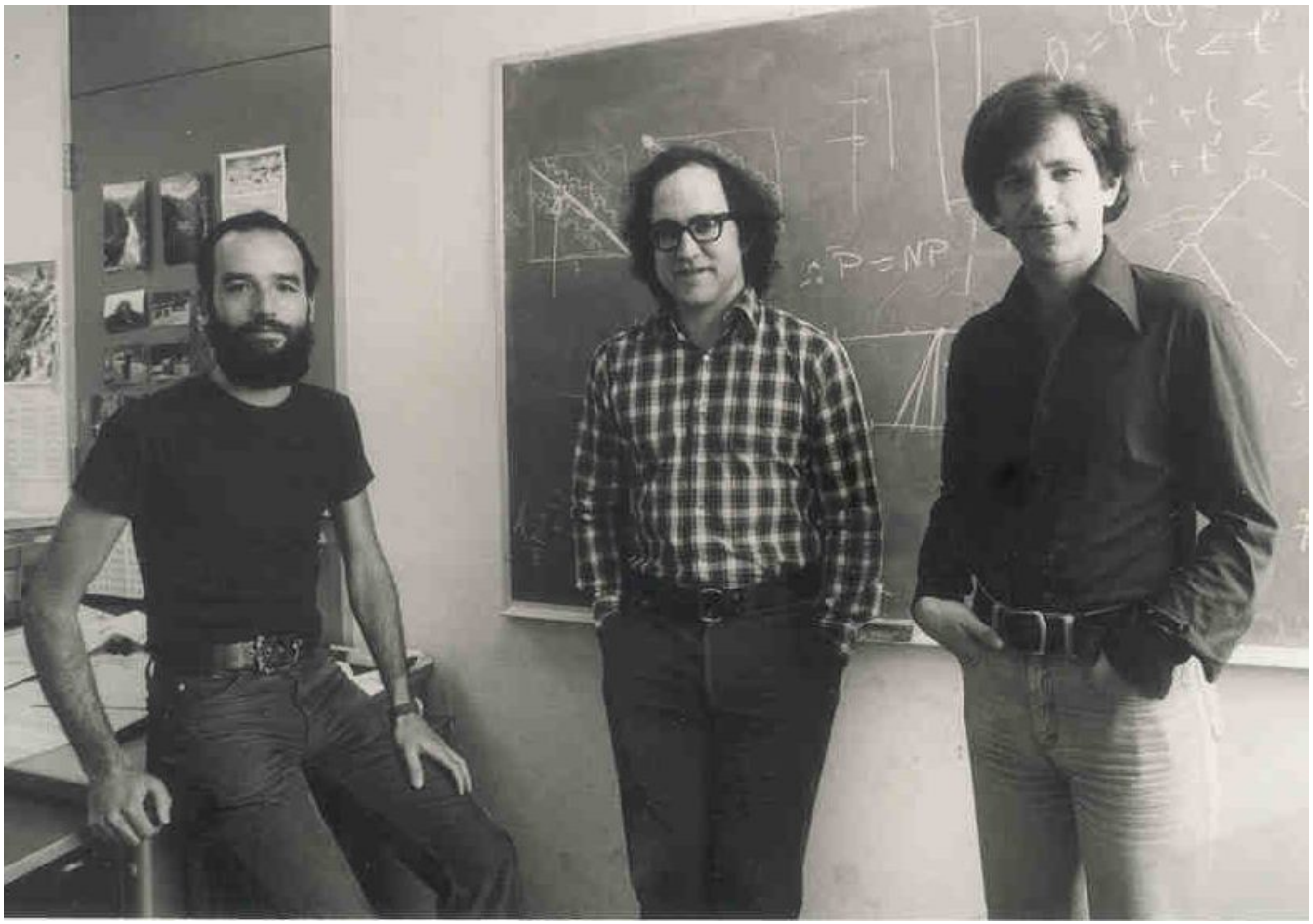


Практическая задача



Если данные не шифровать, то ими сможет воспользоваться мошенник

Шифр RSA



Рональд Райвест, Ади Шамир, Леонард Адлеман

Шифр RSA

RSA-129

1143816257578888676692357799761466120102182
9672124236256256184293570693524573389783059
7123563958705058989075147599290026879543541

Конкурс RSA-129 (1977 г.)

В своей колонке Мартин Гарднер предлагает разложить RSA-129 на множители (и расшифровать сообщение).

Квадратичное решето (1981 г.)

Карл Померанс придумывает новый алгоритм разложения целых чисел на простые множители.

Интернет (1990-е г.)

Параллельные вычисления в сложном проекте можно одновременно выполнять на многих компьютерах

Шифр RSA

RSA-129

1143816257578888676692357799761466120102182
9672124236256256184293570693524573389783059
7123563958705058989075147599290026879543541

Конкурс RSA-129 (1977 г.)

В своей колонке Мартин Гарднер предлагает разложить RSA-129 на множители (и расшифровать сообщение).

Квадратичное решето (1981 г.)

Карл Померанс придумывает новый алгоритм разложения целых чисел на простые множители.

Интернет (1990-е г.)

Параллельные вычисления в сложном проекте можно одновременно выполнять на многих компьютерах

Шифр RSA

RSA-129

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

Конкурс RSA-129 (1977 г.)

В своей колонке Мартин Гарднер предлагает разложить RSA-129 на множители (и расшифровать сообщение).

Квадратичное решето (1981 г.)

Карл Померанс придумывает новый алгоритм разложения целых чисел на простые множители.

Интернет (1990-е г.)

Параллельные вычисления в сложном проекте можно одновременно выполнять на многих компьютерах

Шифр RSA

RSA-129

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

Конкурс RSA-129 (1977 г.)

В своей колонке Мартин Гарднер предлагает разложить RSA-129 на множители (и расшифровать сообщение).

Квадратичное решето (1981 г.)

Карл Померанс придумывает новый алгоритм разложения целых чисел на простые множители.

Интернет (1990-е г.)

Параллельные вычисления в сложном проекте можно одновременно выполнять на многих компьютерах

Шифр RSA

RSA-129 разложено (1994 г.)

Дерек Аткинс, Майкл Графф, Арьен Ленстра и Пол Лейланд $+ \sim 600$ добровольцев $+ \sim 1600$ компьютеров (и несколько факсов) получают разложение.

Ответ

$$114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541$$
$$=$$
$$349052951084765094914784961990389813341776463849338784399082057 7$$
$$.$$
$$327691329932667095499619881908344614131776429679929425397982885 33$$

Шифр RSA

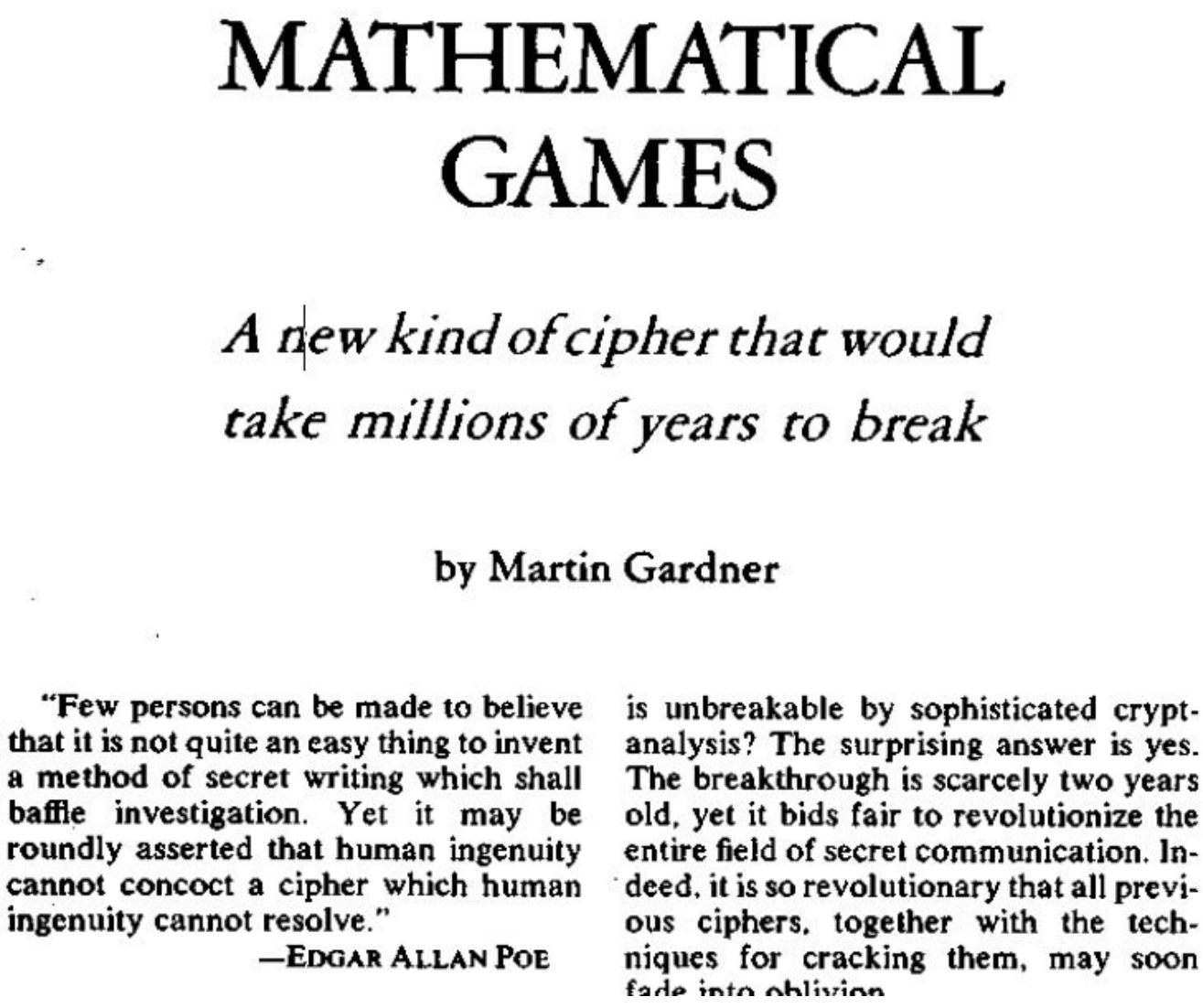
RSA-129 разложено (1994 г.)

Дерек Аткинс, Майкл Графф, Арьен Ленстра и Пол Лейланд $+ \sim 600$ добровольцев $+ \sim 1600$ компьютеров (и несколько факсов) получают разложение.

Ответ

$$
\begin{aligned}
&114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541 \\
&= \\
&349052951084765094914784961990389813341776463849338784399082057 7 \\
&\cdot \\
&327691329932667095499619881908344614131776429679929425397982885 33
\end{aligned}
$$

Шифр RSA



MATHEMATICAL GAMES

A new kind of cipher that would take millions of years to break

by Martin Gardner

"Few persons can be made to believe that it is not quite an easy thing to invent a method of secret writing which shall baffle investigation. Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve."

—EDGAR ALLAN POE

is unbreakable by sophisticated cryptanalysis? The surprising answer is yes. The breakthrough is scarcely two years old, yet it bids fair to revolutionize the entire field of secret communication. Indeed, it is so revolutionary that all previous ciphers, together with the techniques for cracking them, may soon fade into oblivion

Статья Мартина Гарднера

Шифр RSA

The two prime factors of r are withheld, to play a role in the secret inverse algorithm. This inverse algorithm, used for decoding, consists in raising the ciphertext number to another power t, then reducing it to modulo r. As before, this takes less than a second of computer time. The number t, however, can be calculated only by someone who knows p and q, the two primes that are kept secret.

If the message is too long to be handled as a single number, it can be broken up into two or more blocks and each block can be treated as a separate number. I shall not go into more details. They are a bit technical but are clearly explained in the M.I.T. memo.

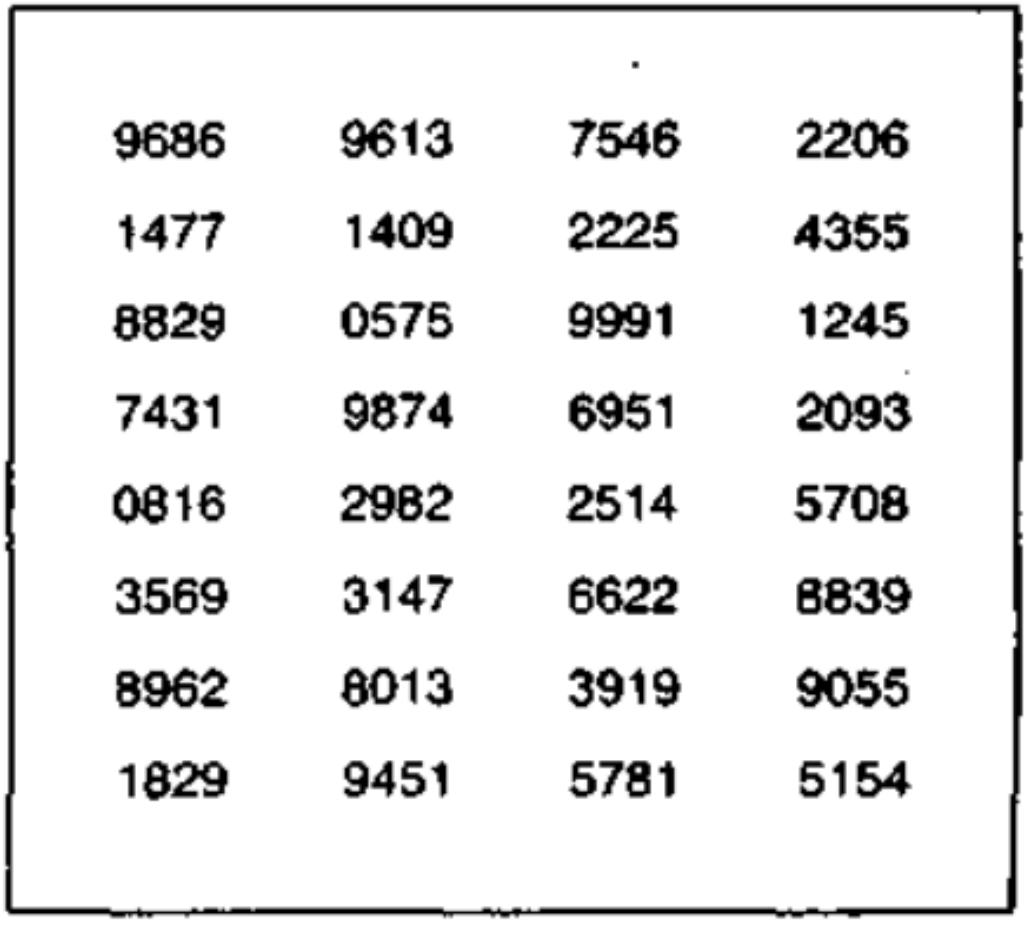
To encode ITS ALL GREEK TO ME, the M.I.T. group has chosen $s = 9{,}007$ and $r = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541.$

The number r is the product of a 64-digit prime p and a 65-digit prime q, each randomly selected. The encoding algorithm changes the plaintext number (09201 ...) to the following ciphertext number: 199[illegible]513[illegible]149780510045231712274026064742320401705839146310370371740625971608948927504309920962672582675012893554461353823769748026.

As a challenge to *Scientific American* readers the M.I.T. group has encoded another message, using the same public algorithm. The ciphertext is shown in the bottom illustration on page 121. Its plaintext is an English sentence. It was first changed to a number by the standard method explained above, then the entire number was raised to the 9,007th power (modulo r) by the shortcut method given in the memorandum. To the first person who decodes this message the M.I.T. group will give $100.

To prove that the offer actually comes from the M.I.T. group, the following signature has been added: 167178611503808442460152071389168398245436901032358[illegible]12178350384469290626554487922371[illegible]4905096786086556624965779748400040570203 73.

Шифр RSA

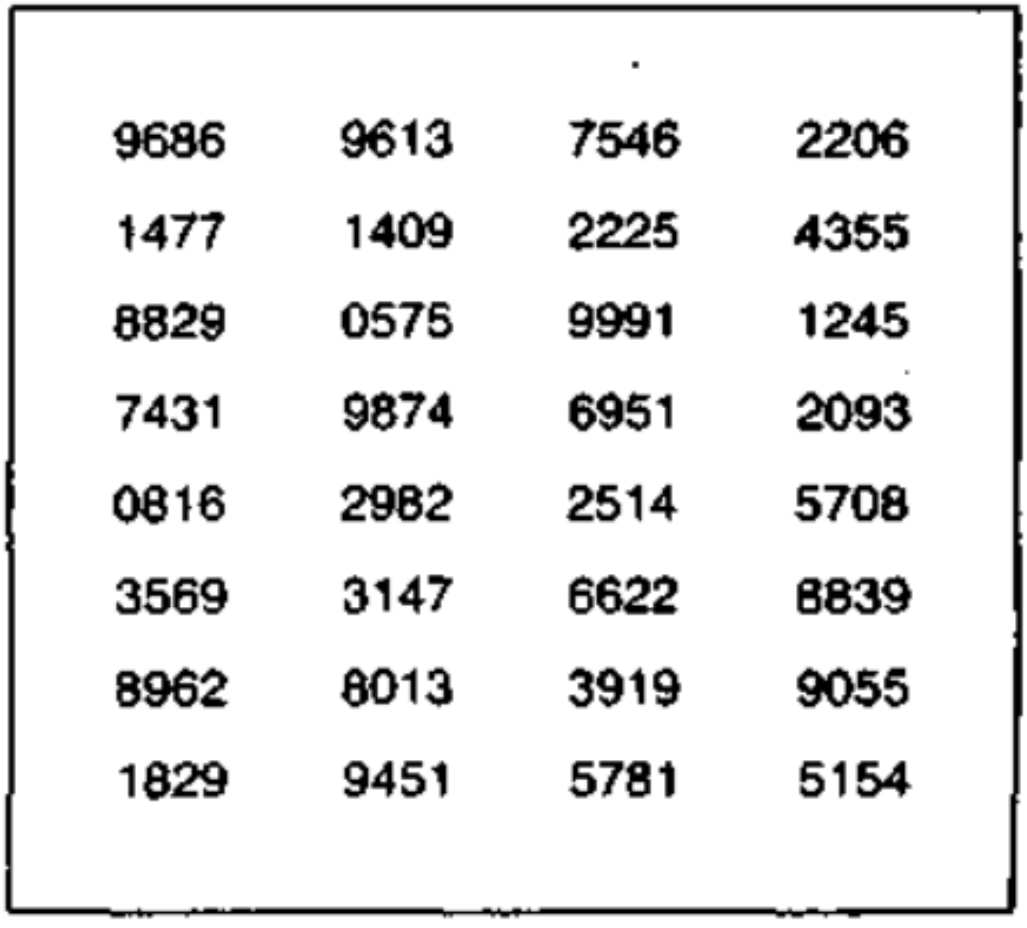


9686	9613	7546	2206
1477	1409	2225	4355
8829	0575	9991	1245
7431	9874	6951	2093
0816	2982	2514	5708
3569	3147	6622	8839
8962	8013	3919	9055
1829	9451	5781	5154

A ciphertext challenge worth $100

Зашифрованное сообщение из статьи Мартина Гарднера

Шифр RSA



9686	9613	7546	2206
1477	1409	2225	4355
8829	0575	9991	1245
7431	9874	6951	2093
0816	2982	2514	5708
3569	3147	6622	8839
8962	8013	3919	9055
1829	9451	5781	5154

A ciphertext challenge worth $100

Зашифрованное сообщение из статьи Мартина Гарднера

Мини-конкурс на шифр RSA

Открытый ключ

$n = 32193888639167989$, $e = 3$

Зашифрованное сообщение

$y = 7868291377216450$

Задача

Расшифруйте сообщение y, то есть, найдите такое 16-значное число x, что x^e даёт остаток y при делении на n.

Мини-конкурс на шифр RSA

Открытый ключ

$n = 32193888639167989$, $e = 3$

Зашифрованное сообщение

$y = 7868291377216450$

Задача

Расшифруйте сообщение y, то есть, найдите такое 16-значное число x, что x^e даёт остаток y при делении на n.

Мини-конкурс на шифр RSA

Открытый ключ

$n = 3219388639167989$, $e = 3$

Зашифрованное сообщение

$y = 7868291377216450$

Задача

Расшифруйте сообщение y, то есть, найдите такое 16-значное число x, что x^e даёт остаток y при делении на n.