Ответы к заданиям — Криптография

Загляни сюда только после того, как сам(а) попробовал(а) решить!

Везде, где речь о буквах, — **русский алфавит, 33 буквы** (А=0, …, Я=32).

Урок 1. Шифр Цезаря

1. **УПЧ** — М(13)+7=20=У, И(9)+7=16=П, Р(17)+7=24=Ч.
2. **ЩШКОНЙ** — П(16)+10=26=Щ, О(15)+10=25=Ш, Б(1)+10=11=К, Е(5)+10=15=О, Д(4)+10=14=Н, А(0)+10=10=Й.
3. **МИР** — вычитаем 7: У(20)−7=13=М, П(16)−7=9=И, Ч(24)−7=17=Р.
4. **ЧИСЛО** — вычитаем 4: Ы(28)−4=24=Ч, М(13)−4=9=И, Х(22)−4=18=С, П(16)−4=12=Л, Т(19)−4=15=О.
5. **ЛОГИКА** (ключ 5). При переборе ключей 3…7 осмысленное слово даёт только k=5: Р(17)−5=12=Л, У(20)−5=15=О, З(8)−5=3=Г, Н(14)−5=9=И, П(16)−5=11=К, Е(5)−5=0=А.
6. **Ключ 8.** Самая частая буква Ц (номер 23) соответствует О (номер 15), значит сдвиг $= 23 - 15 = 8$.
7. У русского алфавита (33 буквы) — **32** осмысленных ключа; у английского (26 букв) — **25** (сдвиг 0 не считается).
8. **Одним ключом $(k+m) \bmod 33$.** Два последовательных сдвига складываются в один; чтобы расшифровать, надо снять суммарный сдвиг.

Урок 2. Шифр Виженера

1. **УУЫА** — Г(3)+Р(17)=20=У; О(15)+Е(5)=20=У; Р(17)+К(11)=28=Ы; А(0)+А(0)=0=А.
2. **КИЮЮШ** — Т(19)+Ш(25)=44≡11=К; А(0)+И(9)=9=И; Й(10)+Ф(21)=31=Ю; Н(14)+Р(17)=31=Ю; А(0)+Ш(25)=25=Ш.
3. **МАТЕМАТИКА** — ключ КОД повторяется К-О-Д-К-О-Д-К-О-Д-К; вычитаем сдвиги 11,15,4,… из Ч,О,Ц,П,Ы,Д,Э,Ч,О,К.

4. **ООРВ.** Ключ ВОД под МАМА даёт В-О-Д-В. Первая М: 13+2=15=**О**. Вторая М: 13+4=17=**Р**. Одинаковые М превратились в разные буквы (О и Р), потому что попали под разные буквы ключа (В и Д) — в этом и суть многоалфавитности.
5. Распадается на **5** шифров Цезаря; в каждую «стопку» попадёт $40 : 5 = $ **8** букв.
6. Длина ключа — делитель 12, кроме 1: **2, 3, 4, 6 или 12**.
7. У Цезаря сдвиг один на весь текст, поэтому частоты букв просто «съезжают», но горб самой частой буквы сохраняется — его сразу видно. У Виженера сдвигов несколько, они перемешивают частоты и сглаживают горб; частотный анализ заработает лишь после того, как найдена длина ключа и текст разбит на «стопки» с одним сдвигом в каждой.
8. **В шифр Цезаря.** Ключ из одной буквы задаёт один-единственный сдвиг для всего текста.

Урок 3. Простые числа

1. **2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47** — простые до 50.
2. $84 = 2^2 \cdot 3 \cdot 7$ (84 = 2·42 = 2·2·21 = 2·2·3·7).
3. $561 = 3 \cdot 11 \cdot 17$ (561 : 3 = 187 = 11 · 17).
4. **91 — составное:** $91 = 7 \cdot 13$. **101 — простое:** не делится ни на одно простое до $\sqrt{101}\approx 10$ (2, 3, 5, 7).
5. Достаточно проверять делители **до $\sqrt{199}\approx 14{,}1$**, то есть простые 2, 3, 5, 7, 11, 13.
6. Простых от 1 до 20 — **восемь**: 2, 3, 5, 7, 11, 13, 17, 19.
7. 31 не делится ни на 2, ни на 3, ни на 5 (везде остаток 1). Это показывает, что построенное в доказательстве Евклида число даёт новый простой делитель вне исходного списка (здесь само 31 — простое) — значит, список простых не может быть полным.
8. Если считать 1 простым, к любому разложению можно было бы приписывать сколько угодно единиц: $6 = 2\cdot 3 = 1\cdot 2\cdot 3 = 1\cdot 1\cdot 2\cdot 3

= \dots$ — единственность пропала бы.

Урок 4. Модульная арифметика

1. $(23+19) \bmod 7 = 42 \bmod 7 = $ **0**.
2. $(8\cdot 9)\bmod 5 = 72 \bmod 5 = $ **2**.
3. $(9 + 20)\bmod 12 = 29 \bmod 12 = $ **5** часов.
4. **7** — обратный к 4 по модулю 9, потому что $4\cdot 7 = 28 = 3\cdot 9 + 1 \equiv 1 \pmod 9$.
5. У 6 нет обратного по модулю 9, потому что $\gcd(6,9)=3\neq 1$. Все кратные 6 по модулю 9 дают только 0, 6, 3 — единицы среди них нет.
6. $2^{10} = 1024$, а $1024 \bmod 1000 = $ **24**.
7. **4.** Так как $3^6 \equiv 1 \pmod 7$, а $100 = 6\cdot 16 + 4$, то $3^{100} \equiv (3^6)^{16}\cdot 3^4 \equiv 1\cdot 3^4 = 81 \equiv 4 \pmod 7$.
8. Если $a\equiv b \pmod m$, то m делит $a-b$. Тогда $a^2 - b^2 = (a-b)(a+b)$ тоже делится на m (первый множитель делится), значит $a^2 \equiv b^2 \pmod m$. ∎

Урок 5. Обмен ключами Диффи–Хеллмана

1. Смешать две краски легко, а разделить смесь обратно на исходные цвета практически невозможно. Эта «односторонность» и позволяет обмениваться смесями открыто, не выдавая секретных красок.
2. $A = 5^2 \bmod 23 = 25 \bmod 23 = $ **2**.
3. $B = 5^2 \bmod 23 = $ **2**; общий секрет $= B^a \bmod 23 = 2^2 \bmod 23 = $ **4** (то же даёт $A^b = 2^2 = 4$).
4. Открыто: **p, g, A, B.** Секретны и подслушивающему неизвестны a, b и сам общий секрет.
5. **Задача дискретного логарифма** (найти показатель a по известным g, p и $A = g^a \bmod p$).

6. При большом p дискретный логарифм невозможно вычислить перебором за разумное время, тогда как при $p=23$ секрет находится мгновенно. Большое p и обеспечивает стойкость.
7. Оба вычисляют одно и то же число $g^{ab} \bmod p$: Алиса как $(g^b)^a$, Боб как $(g^a)^b$. Поскольку $(g^b)^a = g^{ab} = (g^a)^b$, результаты совпадают.
8. Идея атаки «человек посередине»: злоумышленник перехватывает канал и договаривается по Диффи–Хеллману **отдельно с Алисой и отдельно с Бобом**, выдавая себя каждому за другого. Тогда у него общий секрет с обоими, и он читает (и подменяет) все сообщения. Защита — подтверждать личность собеседника (например, цифровой подписью из урока 7).

Урок 6. Идея RSA

Ключи из урока: $n = 33$, $e = 7$, $d = 3$.

1. $n = 3\cdot 11 = $ **33**; $\varphi = (3-1)(11-1) = 2\cdot 10 = $ **20**.
2. $7\cdot 3 = 21 = 20 + 1 \equiv 1 \pmod{20}$ — значит, 7 и 3 взаимно обратны по модулю 20. ✓
3. $c = 8^7 \bmod 33 = $ **2**.
4. $m = 2^3 \bmod 33 = 8$ — исходное число вернулось. ✓ (Проверка: $8^7 \bmod 33 = 2$, затем $2^3 = 8$.)
5. $c = 10^7 \bmod 33 = $ **10**. Забавно: число зашифровалось само в себя (это редкая «неподвижная точка»; в настоящем RSA с большими числами такое почти не встречается и не вредит стойкости).
6. При $p=5$, $q=11$: $n = 55$, $\varphi = 4\cdot 10 = $ **40**.
7. Все вычисления идут по модулю n, поэтому результат — это остаток от 0 до $n-1$. Если $m \geq n$, разные сообщения давали бы одинаковый остаток, и однозначно расшифровать было бы нельзя.
8. Чтобы найти d, нужен $\varphi = (p-1)(q-1)$, а для него — разложить n на простые p и q. Факторизация большого n практически невыполнима,

поэтому d вычислить не удаётся, хотя открытый ключ (n,e) у всех на виду.

Урок 7. Хэши, пароли и цифровая подпись

1. Главное отличие: шифрование **обратимо** (расшифровал ключом — вернул данные), а хэш **односторонний** — по нему исходные данные восстановить нельзя.
2. **Односторонность**, **лавинный эффект** (малое изменение входа полностью меняет хэш) и **стойкость к коллизиям** (трудно найти два входа с одинаковым хэшем).
3. Потому что при краже базы утекут только хэши, а из них пароли не восстановить. Сайт проверяет вход, сравнивая хэши, и сам пароль хранить не обязан.
4. **Соль** — случайная строка, добавляемая к паролю перед хэшированием, своя у каждого пользователя. Она защищает от заранее заготовленных таблиц хэшей («радужных таблиц») для популярных паролей.
5. Потому что к каждому «qwerty» добавляется **своя случайная соль**, и после хэширования получаются разные строки. Одинаковые пароли в базе выглядят по-разному.
6. Создают подпись **закрытым** ключом автора, а проверяют — его **открытым** ключом.
7. **Не пройдёт.** Изменённый текст даёт другой хэш, а подпись сделана под старым хэшем. При проверке два хэша не совпадут, и подпись будет признана недействительной.
8. Хэш — короткий и фиксированной длины, его быстро посчитать и подписать одной операцией, тогда как подписывать длинный документ целиком медленно и неудобно. При этом хэш надёжно «представляет» весь документ: изменение любой буквы меняет хэш, так что защита целостности сохраняется.