МАКЕТ

А.Н.Кабанов, Е.Г.Кукина, В.А. Романьков

Задачник по криптографии

Задачник к учебнику В.А.Романькова «Введение в криптографию».

Адресован студентам, впервые изучающим криптографию. Может также оказаться полезным специалистам в данной области.

Задачник подготовлен при поддержке Министерства образования и науки Российской Федерации, проекты 14.B37.21.0359/0859.

1. Платформы шифрования

Задача 1. Восстановите первую строку одной из наиболее известных шифровок на русском языке: «...

Его мы очень смирным знали,
Гроза двенадцатого года,
Но бог помог – стал ропот ниже...»

Задача 2. Восстановите начало одного из самых известных монологов на английском языке, зашифрованное простой заменой букв на числа:

$$11, 17\_3, 7\_17, 10\_0, 17, 11\_11, 17\_3, 7\_$$

$$\_11, 21, 23, 11\_6, 8\_11, 21, 7\_20, 5, 7, 8, 11, 6, 17, 0$$

Задача 3. Что помогает при расшифровке? Сколько в английском языке слов из одной буквы? Из двух букв? Объясните, почему зашифрованный текст лучше записывать без пробелов и без знаков препинания.

Задача 4. Испанский алфавит состоит из 29 букв. Ниже дается оцифровка начала одного из известнейших стихотворений испанской поэзии:

$$5, 14, 18, 9, 28, 0\_5, 12\_13, 0, 15, 22, 17\_$$

$$\_4, 5\_12, 0\_7, 23, 9, 22, 0, 20, 20, 0\_$$

$$\_21, 5\_20, 17, 14, 18, 5, 15\_12, 0, 21\_2, 17, 18, 0, 21\_$$

$$\_4, 5\_12, 0\_14, 0, 4, 20, 23, 7, 0, 4, 0$$

Можно легко восстановить текст по испанскому алфавиту. Заметим только, что у него есть варианты.

Следующая строфа – перевод этого текста на русский язык, принадлежащий М. Цветаевой:

$$10\_4\_6\_11\_4\_4$$

В ней указано только количество букв в словах. Приведите эти знаменитые строки!

Задача 5. Имеется достаточно длинный литературный текст английского языка. Текст зашифрован методом простой замены. Взломщику разрешается узнать кодировку любой буквы по его выбору. Как он может узнать кодировки сразу двух букв? Какие это буквы?

Можно ли с большой долей вероятности узнать три буквы, если разрешается выяснить замены только двух букв?

Задача 6. Во время 2-й Мировой войны некоторые из американских солдат, чтобы указать место своего пребывания (открыто писать было нельзя – письма просматривались), меняли на конверте второй из инициалов адресата, например, писали вместо “A.B. Smith” – “A.T. Smith”. Буква “T” означала первую букву места дислокации. Затем в следующих письмах появлялось “U, N, I, S”. В итоге родные должны были все это заметить и прочитать ”TUNIS“. Объясните, почему все-таки часто это не срабатывало, хотя родные и понимали идею.

Задача 7. Алфавит русский (33 буквы). 1. Какой номер при стандартной оцифровке имеет слово ОПЕРА, ВОЯЖ?

2. Какому слову из 4 букв соответствует номер 14784? А номер 7425?

3. Какому слову соответствует номер 317? а номер 591775? Можно ли ответить однозначно и почему?

Задача 8. Алфавит английский, 26 букв. Какой номер при стандартной оцифровке имеет слово SMART?

2. Модулярная арифметика

Задача 9. Используя обобщенный алгоритм Эвклида, найти

$19^{-1}(\mathrm{mod}26)$, $131^{-1}(\mathrm{mod}834)$.

Задача 10. Используя лишь калькулятор, найти число x, удовлетворяющее уравнению

$$3^x = 5(\mathrm{mod}p),$$

где $p-1 = 2 \cdot 3 \cdot 101 \cdot 103 \cdot 107^2$.
Упрощенный вариант: $p-1 = 2 \cdot 3 \cdot 101$, или еще проще: $p-1 = 2 \cdot 3 \cdot 11$.

Задача 11. По Китайской теореме об остатках вычислить x (найти общее решение) для следующей системы сравнений:

$$\begin{cases} x &= 5(\mathrm{mod}7), \\ x &= 3(\mathrm{mod}11), \\ x &= 10(\mathrm{mod}13). \end{cases}$$

Задача 12. Используя Китайскую теорему об остатках, вычислить x (найти общее решение) для следующей системы сравнений:

$$\begin{cases} x &= 1(\mathrm{mod}15), \\ x &= 3(\mathrm{mod}17), \\ x &= 3(\mathrm{mod}24), \\ x &= 4(\mathrm{mod}19). \end{cases}$$

Существует ли решение, если вместо 19 взять в качестве последнего модуля 18?

Задача 13. Сколько существует обратимых матриц порядка 2×2 над кольцом $\mathbf{Z}_6$? Над кольцом $\mathbf{Z}_8$?

3. Элементы шифрования

Задача 14. Пусть алфавит состоит из 26 букв английского языка. Шифрование осуществляется при помощи подстановки

$$s = (p, h, u, q, l, f, e, r, m, g, y, x, v, s, n, i, b, o, j, c, w, t)(a, k, d)(z).$$

Здесь подстановка определяется циклом, в котором буквы переходят в следующие по написанию, а последняя буква переходит в первую (цикл замыкается). Буква z остается на месте.

Пример: исходный текст – *I am fine* = *iamfine* (мы не учитываем пробелы и разницу между строчными и прописными буквами, а также знаки препинания), шифрованный текст *bkgebir*.

1) Зашифровать текст:

Some people say a man is made out of mud A poor mans made out of muscle and blood Muscle and blood and skin and bone A mind thats weak and the back thats strong Sixteen tons.

2) Расшифровать текст:

btkiarmpumjqyurkwuwukmprmranpmrrpirdmtur mrpurwukmprmrapukgrnajrnefjtkgkmdbirsrmxek wrbgrrpgkmdnjetrkdrirnngkmdnjetjrofkdrfjiaji.

Задача 15. Алфавит русский (33 буквы). Исходный

текст разбит на блоки величины $n = 8$. Буквы внутри каждого блока меняются местами перестановкой

$$s = (1, 8, 2, 7)(4, 6, 5, 3).$$

1) Зашифровать текст:
Скучно на этом свете господа Гоголь.
2) Расшифровать текст:
алмрпотуевиидкчьдубъуичиьнслтактишыувбгазнваонинийсекнсе.

Задача 16. Алфавит русский – 33 буквы. Разбит на блоки величины $n = 8$. Буквы внутри каждого блока переставляются перестановкой:

$$s = (1, 6, 4, 8, 7, 2, 3)(5).$$

1) Зашифровать текст: *Все студенты ушли на субботник кроме Михайлова*
2) Расшифровать текст: *Воскресенье будет коротким*

Задача 17. Зашифровать текст с помощью гаммирования, переводя все его буквы в бинарные последовательности длины 5:
hidden number is a key = 7 8 3 3 4 13 ....
Выбрать в качестве ключа свой индивидуальный номер, записанный в двоичном исчислении. Индивидуальный номер равен сумме значений букв

фамилии (русский язык, 33 буквы, стандартная нумерация).

Задача 18. Назовем шифр замены, отвечающий подстановке $\sigma \in \mathbf{S}_n$, *гомоморфным*, если он удовлетворяет тождеству

$$\forall i, j \in \mathbf{Z}_n \ \sigma(i+j) = \sigma(i) + \sigma(j) (\mathrm{mod} n).$$

Сколько существует гомоморфных шифров замены при фиксированном n? Как они устроены?

Задача 19. Следующая шифровка получена шифров сдвига в английском алфавите A-Z. Пунктуация соблюдена, сдвиг применяется только к буквам.

1. Jr frjrq n fzvyr ba n ubefr'f nff, naq n lrne yngre vginf ryrpgrq Cerfvqrag!

2. Dbksvobc pyb pkvo yb boxd byywc dy vyd pspdi moxdc xy zryxo xy zyyv xy zodcs ksxd qyd xy msqkboddoc.

Расшифровать!

4. Элементы криптоанализа

Задача 20. Пусть некоторый английский текст зашифрован методом простой замены. Предположим, что определено значение, скажем 14, буквы q. Пусть в тексте содержится сочетание 14, 18. Чему скорее всего соответствует 18?

Задача 21. Пусть известны шифровки $c_1 = E_{\tau_1}(m), c_2 = E_{\tau_2}(m)$ одного и того же достаточно длинного текста m, полученные шифрами перестановки с одинаковой длиной l блока: $\tau_1, \tau_2 \in \in \mathbf{S}_l$.

Как можно с помощью этой информации эффективно найти l?

Задача 22. Пусть имеется исходный текст m и его шифровка, полученная с помощью шифра замены: $c_1 = E_{\sigma_1(m)},\ \sigma_1 \in \mathbf{S}_n$.

Найти m можно частотным анализом или еще каким-либо способом. Вопрос в том, облегчает ли задачу знание еще одной шифровки того же текста: $c_2 = E_{\sigma_2}(m),\ \sigma_2 \in \mathbf{S}_n$?

Задача 23. Назовем шифр замены, отвечающий подстановке s на n символах, гомоморфным, если он удовлетворяет тождеству $s(i+j) = s(i) + s(j)(\mathrm{mod} n)$.

Допустим, используется английский алфавит из 26 букв со стандартной нумерацией. Пусть задан

гомоморфный шифр замены, соответствующий подстановке $\sigma \in \mathbf{S}_{26}$. Можно ли полностью восстановить σ, зная $\sigma(b)$? Тот же вопрос для $\sigma(c)$. Что можно сказать по этому поводу в общем случае?

Задача 24. Допустим, что вместо буквы "A" английского алфавита, частота которой $8,2\%$, используется 82 различных знака с равной вероятностью. Вместо "J" частоты $0,1\%$ – 1 знак и т.д. Таким образом в алфавите появляется не 26, а 260 букв. Но теперь они встречаются в тексте с приблизительно равной вероятностью. К такому тексту применяется простая замена. Покажите, что в этом случае частотный анализ по-прежнему эффективен, только применять его нужно по другому. Каким образом?

Задача 25. Расшифровать текст.

1) *шйфщъсюупыфпхзэчйфйхйзгяёвефнйъсеушдзэд фсьчйусшйффпдйндчевйфрпвйфйбрпеъейфщъеы йфдфдгчсыкгсщсшсчеэксмнбсзэсдшзвснсщчйф еыешйюзкыйцдшздщсбдвъйчйредазшсехяфешдч зеэдэзвехгсуфйфеасгчдзэягъдфееефйвйуйфе евйобпаеуфехъдуязъсшфсуфйдэыэсъфэсъзэса йшэсччснйфйшсафйенечнфсщедъедщсыеэйъебч*

ящсашсгчсзвсдвэсфйзъпёйфсьйгыдхсшддзъеш
йнгсшдудээзсьдздбфевснэсшпзнсодэдгдчднс
ъшеэкзюсшбфйъсвсшдейъяфефдгсщсшсчеэксфп
фдёфехгезйэдъюхинещчйфэйхыэсвйзйдээзюгяё
вефйэсгсуфйфеювйвгчйшеъсзвябфпэднябешеэ
дъкфддыэсяодзгдчшпхнефяэнсдщсгчедубйшвй
фйбядцдшйичсгсчэянсфчдйъююязъпёйъзэчсмп
дшщдфеюсфдщефйеуязээсшзднфдчсззеазвсщсе
ъезсшдээвсщсинещчйфэйебйодыдъсшдвйфденд
шёдщсэсщбйшбдшюфсзэснщсбяфевйвехзшюудаз
эйвенеинещчйфэйнейгчсмдззсчйнйэднйэевея
фешдчзеэдэйнйвщеъъшпхсбрйеужофсаймчевег
съяыешёдщссьчйусшйфедшвдньчебодбесфйщеъ
кбдфхдауйчйззвйоясьсшзднгсгсчюбвяюгсъяы
еъгчещъйёдфедгчсмдззсчзвсаыдэпфйчйафйев
йфэпщягэйгчедхйэкфйбшйндзюрйшшеффегдщез
сшндзэфсгсчйьсэйэкфйбчюбснфйяыфпх

2) *pehjdziavahrazketakefakgayacaypzjpkefakg ayjlvjprqyajllpsaalkgjkqilerqdfiptarksyq adzqujdktalqacakgqruehlztakgaadzqkleemrj rkgehfgpehjyalakkqdffejdzqsqkryajlvallqz edkvjdkkemdevzedkrnajmqmdevxhrkvgjkpehya rjpqdfrenlajrarkenaonljqdqdfzedkkalliauj hraqkghykrzedkrnajmqmdevvgjkpehyakgqdmqd fqzedkdaazpehyyajredrzedkkalliaujhraqkgh ykrehyiaieyqarkgapujdtaqdcqkqdfthkreiajy ajlkefak-*

gayiqfglpsyqfgkadqdfjrvazqatekgp hehjdzqvqkggajzqdipgjdzrqrqkjdzuypzedkrn ajmqmdevxhrkvgjkpehyarjpqdfrenlajrarkena onljqdqdfzedkkalliaujhraqkghykrzedkrnajm qmdevvgjkpehyakgqdmqdfqzedkdaazpehyyajre drzedkkalliaujhraqkghykrqkrjlladzqdfqfek kjrkennyakadzqdfvgevajyapehjdziaqujdraah rzpqdfjyavazedkrnajmqmdevxhrkvgjkpehyarj pqdfrenlajrarkenaonljqdqdfzedkkalliaujhr aqkghykrzedkrnajmqmdevvgjkpehyakgqdmqdfq zedkdaazpehyyajredrzedkkalliaujhraqkghyk rzedkkalliaujhraqkghykrqmdevvgjkpehjyarj pqdfrenlajrarkenaonljqdqdfzedkrnajmzedkr najmzedkrnajmdeqmdevvgjkpehyakgqdmqdfjdz qzedkdaazpehyyajredrqmdevpehfeezqmdevpeh feezqmdevpehyajlfeezeg

3) *zphqaqpavqzmjmhmykzhmiqpsnpbhsimapprhmyzhmiqpsnpbh szlvqmyiuvppihszlvqmyiuvppimyizgkymyiupyqmhkyindmn zoqmgmyindqumlgkzznrpytjpsvpmizkfnqqynpymyiodmnipj pstqnmypndqrimjpviqrmyiiqqaqrkziqunpdurpndqripynjp slmvvhqlmszqklmyntpkpoqhjzpsvnpmlphamyjznprqkomzup rypyqhprykytodqyndqzsyikiynzdkyqkaklgqisahjzdpeqvm yikomvgqinpndqhkyqkvpmiqizkfnqqynpypbyshuqrykyqlpm vmyindqznrpytupzzzmkioqvvuvqzzmhmzpsvjpsvpmizkfnqq ynpymyiodmnipjpstqnmypndqrimjpviqrmyiiqqaqrkziqunp durpndqripyn-*

jpslmvvhqlmszqklmyntpkpoqhjzpsvnpmlpha myjznprqoqvvkbjpszqqhqmlphkyuqnnqrznqamzkiqmvpnpbh qyikiynmvpnpbhqyikqipyqbkznkzkrpyndqpndqrpbznqqvkb ndqrktdnpyqipyntqnjpsndqyndqvqbnpyqokvvpdurpndqrip ynjpslmvvhqlmszqklmyntpkpoqhjzpsvnpmlphamyjznprq

4) *ПЩИМИЙЛЬМЪГПРЧГГЪЖМГХЪЧ ДЛИКЩПЛПАБКОЬКЛШГУИЖИГГЪЖБ РЫЗИЙЛЯЛЕТЙСЩЪДОДСЕЖЦЫКЕ ТРПЭМЙПАЪЪСЭЫАЦМОЫРЛДЦЫАИ ЖЖЫЫРЧЛЯЛУНЛЖЯЖЬЯЫКЦТЙЖОЯ ГЫДВЪЖЯСАЪЧРИЛРЕРХЛЙШТЦЩ ЙЫНСИИДФЦПЩЪАДЪИПЛШЛХКЛШЦ ЕЖЫКЛХЪОУПРСОДОРТЮУФИДРЦ ЯЖИТАКЦСЩСРЛЧИШЛЦЪАДЬХЧГБ ЪЪФЖВКЦТМАЛМСАВЮХЖАКЛЙГО ЬГРТЮРНЩДЛШЦМСАГПФСОГНЙС НДГРТОГЗИУЦИНШЧФБЗЙЖЫКВЖБ АВЪПУЛЭАЧЦЛМЛЙГОСГУМТАТФ ЭРУЪЖЕПУПРСЪАЭЯЛГУЛЩЪВХНГ ЖЪХЛМШИЫЖРЫЬВЖНХТУПМЙЛКЛУ МЛЦБИИЮВВНЙОВЕЦТЙШНЬГРГК ИФЬЫЫЙЖЙШНМЦЮЫЫИЧТЭОРЕАВЪ ЖХЫЧАЧЕЯСЯЛФЪЫБЗСВСАЧМИД ЬИЙИФЭЩЧРКЪИПГБККДЯЧКЩООЫ*

ИНКЛШЪЛБГЭЪЛБГЩЖЛЧЛГОВЙР
ВЩШСОУТЩЙЛГПШЪЪЫНДЕГВБВЪО
ЯНЙМЮЧРЖХРЖПРЖААЪЛБГОПСЪ
ЙАНМТОСЬЕТЖДЫИЕОЧАХТЮСЖЛ
ЖНСДПЖГУЪЖИЮДЪЛИЕССЕЛЮДЮЖ
ШГЫРЛМРИОТМНСРЛИРУЮЖШТФПМ
ЖАКАЛДЕЬЫЦЖМСАНПГБДЛКЕЬЫ
ЦТЩЮБГЖЬВЗЙСЫХЛЙСППЬОЬСА
ЛЕТУЛРЕТЖОРДГЫГГЖАГПЕЧГН
БИУИОПТДГДЫКПГЯЛЧЦАСБЛИТФ
БЛЩЪДКЙЛМВЪИПЛШОЬТНВКУТЩ
ОБЖЧОЬГЦШРМКЦЪЗДЯЖИРЭЩИДР
ППМЕЙСГЦШРУПЦЛНИЛЯЖОДПЕМ
НВВЖШЕЫЬЧУВСГРЕАВШИЧГУЖЖ
ФОВЖЖФОЩАЧЗЮВЫМСВЩАЧЗЮВЫМ
СВУПДЕРПЪЖИРХНМЧФКЛЦЦПХЦУ
УТЯБЛПОСЫМЙТКНРТНИТЙСБХЛ
ТЧПЭПВЪВЭНФХГЖИЧХГЖИЧМНВВ
ЖШГУКЩЙГЯПЕЖЪГЫЧЙЛОПСЪНИ
ПМЖЦСРЖМРЖЦЕЖЛХЛТЧФШОЙОО
ЫЖРИТПЛЙИГШЪНШЫЮЕЩЪМВЪЛХЖ
ЫАЖЦГАШИШНСЬЪХЪНБЭЪОСЫЛИ
РУЭЙЭТИЯЧФТХЫИФЕВЪЙЖОДЬЪХ
ЙПРЙЫЕСЫВСУУПТЦЪДФЪСЪДСЛМ
РУОИЙЛШЪЧРФСДКЕИШЯЙТОДАЕ
ЪЧХЛСЪО

5) *ЕАСЗУВНУВРДУАЙЪББВФЪЙХТВ*
АЙЪББВФЪЙЪКВЙПЪАХБЕУДАСЗТДЗ
ХРУСТМЙЪФЪЙХЭУХЦХДРЩХМХУЕ
ЩПУДТХБЕХМПЕУДУАСЗЯЩХЭИЗ
ВЮЩПЖЕТХЗХФАСЗЩХБФВЪББЗГМЮ
ЦЙЪМДЗЪЮХЮУСЮЗХИУХЮУВЮЩЪ
ЮЩГРВЗЪЦЪЙЦЪИТДЙНЗСЭБЙГУЩ
ЙДАЕЩВИЦВЗСИВЗЪЙПЕУХБЙГН
ЪЗЪЩВРЦЪРДЙДНЦЙВЭВЕЧХФЪЗУ
ВФЦХЩЗХИВУХТМХЦЙЪЦЪИВЗФВ
ИВЭФВИВЭЪТХЛДЩЮЩВЗАСЕТДЙ
НВИКДТЦХБФВАХФЪУЪНЩДЧЙДАЕ
ЩЦХТУДМХЩЙВМГУДМХФУЕЗЮЕБХ
ЗГАХБЗВНЪГБЗХИВЩУДФДЫДИЪ
ЮЦВНВЗХУИУЕЩУХИТХЪБЗВНВЮТ
ХЩЙЕИГМХЙЪМХФМХЗХЭДБХАГЫ
ЗВЩВАЗДЮУГЗХЩЩХРДУУСЭЩХМХ
ЙУДХЩГБЙХНСХЙХАДЗЕЩВТЛЪН
УПИЮДБФВУВИХЗХЮЦДИЦХУКДЦХ
УКХИФХЫЗХАФХФДЗВНВАГЙУЪЦ
АСЗИТХДЭЙГЦДУХЮЩВЗХЮЩЙВЫУ
ХХЩЩХБХТУДРЩХЯЩХАСЗЩХИВЙ
ЪШТХЭЕЪЮДБХФУЕЕЮУХМХТУЖЮ
ГЙХИСЭИНБЗЕФДБХМЙЕТХЭФЙГН
ПЕТХЪИЗЪЧЪДЮЙХЦЪИСАСЗЪЮЪЗ
ПУСТЪЗЖФПТЪЮМВЮЪАХИВТНВЩ

ДГЙХЦЪГЙХЦЪБУДИВЪЗЖАИЪВУ
ВЩХЗЪЭЛЪБГЗЪУ

6) *ДЮМНЗРЛЮЬДСЬЗЕЮТЪШАЬЛР*
ЗПЗВЮНМЮЬЛСАПСЕСЖДШЩЭНЗЙШНТ
ЩЬТВЮРКАРШБЗПЛШАЬЛРЗЮЛВТЬ
ЬДЮАЖСВДРШЮЛЙСЛЗЙДЮМНЗЧВ
ШПСРЬДЗИЬЛЮЙШЖЗБЗЪКРРСЙШ
ХШСЬРЮСДЗДЮЧУИПСРОЗИЪЙТНП
ШЖЗПСБПЗЙЗДЛЮЪСВСЛССЕПСМ
ЮЙЮЬЪКЙЮПБРЗЙТЛСОПЮЮПМЮРЮ
ВШЙШНШЬЯНЗЮЬЛЗРУЬРЮАДВЗА
МЙТЩЮАШМВСОПКАЮЬЛЗРУВЮЬЬШ
ЯПЗРЬСМНЗИДВЮРУЮЛВТДЛРЮШ
ЩЮЛЕЮЯШБЬСВНЖЗРКПТХСВПКАЬ
ЛКНИПЮРКЕШЕСПСЕЧЮДВЮЯЪЮЙУ
ЧЮВЗЭСПШАШЮЪШНПЮВЗРПЮНТО
ПЮШЬЧЮДЮАПЮВТДЗЕШИБЗЕДПТ
ЙЗЬЙТЩХЛЮЪЫЛЮАВСХУЯПСНЮЬЛ
ЮАПЮАПСЮЬДРСВПШЙЬИЬДЮВЪ
ПКАНТЩЗППЗЗЩЕЗЛЮРЗХСВПССЛН
ЮВЮМЗЧВШЕЮВЬДЮМЮЬЗНЗЭСЙЛ
КШЬРСЭШГЮПЗВШИЮХСПУЬЧЮДЮА
ПЗИЛЮЙУДЮПСПЗНЮЬЮЕПЮЯЮПСЕ
МЮРЮВШЛУЛКЕШЙКАШРСВПКАЕК
ЪТНСЕНВТБУИЕШМТЙИЛУЖСЙЮР

ЗЛУЬИЬЛЗВСЛУШЙСМДШСЕСЬИЖК
ЪТНТЛПЗНПЗЕШДЗДЬПСЭПКСБР
СБНКЙСЛСЛУЗППЗЗЩЕЗЛЮРЗЮНП
ЗШБЧСЬСПДЮЛЮВКСШЬЧЮЙПИЙР
СВЛШПЬДША

7) *ЯРЯЩЮФЮЙАИЯЮЕВЫБКЫЙЮЪШЭК*
ЭЦИРЪЛЯЭЩББТЮНБЯАЖЙБФБИИЮГ
ВДОЯЭЙЮФЫЬЮЕИБИРНЭКЭЮВЮЯЮ
ЕЙЮЕЙИЮТЮИБШБФБИЯЮТШРЯЮИП
АКЫЩЯРМАИБВБПРФЫИЮПОЮШЭКА
ЙЮБЕИБОИРЩЛБОБГВЮЕШЭШЮНЮТ
ЮЕИБШРФЫИБЕВЮЩЙЮОНБОЫЯРЯА
ТНРЪОШБОАИРЯЭЩОРЖЦРЗЛБОРБ
ОЯНДМЮЛИАЯАЛБЦЭОЯАНВАПАЦР
ЮТНРШЮЕЯОЮОДЬНРОЙЮЕАФАФЪЬ
ЮЛИАЯГИБВЮЙИЪАВЮЙИАОЫИБИР
ШЮЯРЯЩЛБОФЮЦШБЩЫАЯРЯЬБЩВН
АЪОИЮЮОШДЖРБОЭЩОРФЮБОБФЮР
ВНЮЖЮМАБШЭЙРЪОЩЙЭОИЮЛБНИЮ
ОЮФЫЯЮЛПБНРЮЛШЮЛБФРРИИРРЖ
ЙРОЮЛРГВЫЪЦРНРЦЮНБИИДЕШЮЙ
ЦРЦФЭЪМАЦИЫЙЮЪЦРЮШАИЮПБЩО
ЛЮЛШЛЮБЙАЦРОБЬГГВЫЪЦРФЮМЫЙ
БИГВНБШРЛКАЖТЭЬЦРЙБНОЛДЕЖ
ЮФЮШТФРЦЦРОЮПОЮЙАНМБЩОЮЯАТ

НЭЬЦРОЮПОЮЬЮТИБЩВРЩРИИРРЖЙ
РОЮЛРЯЮТШРГИЮПЫЪМШЭББВНАЖ
ЮШРМАЦИЫЯРМБОЩГЛАЩАОИРЛЮФЮ
ЩЯБПОЮВЮПБЩОАПОЮЪИЮЩОЫПОЮ
ЩЛЮЬЮШРВНБШЙАФЮЕТЮЩОЫБЕЩШ
ЭШЮПЯЮЕЛНЭЯБАЛЮОЛЮКФРЮООЯАИ
ЭЛВЮЯНДЛРФЮЛИАЙРОБФЫИЮЛЦТФ
ГИЭФРИРЙБИГБЕТЮЛЮНЪОДФЫШР
ИОЭШАЯОЮЛРФРЩОНРИАЗДРШРЮО
ЛБПРБОГРИИРРЖЙРОЮЛРЙЭЦР

8) *ЛРЛСДЦТФКАААЬЧЙЙСЦПЛЮЙЫОЦ*
ИТЫФЦКСЫФХОЙШСГЙСЙЛЖНЩЩОУЧ
ХАЛОЗГЫУЯБХАФСЧМАЕСБЦЯЕУЗ
ДЕОЧЙГАВЙЯТЫЛЫБРОЧЦБОЩЖХЗ
ЙХЕЦНГЦХПЬЫПЛХЖТЫЛЫБСЦЧЧИ
ФОРХКЫЦШХЫХРОСТТРФМНТЫУТГ
ЖУУМОИЬМИШТЯЛСЙМЧНЖБСЦШРК
СЬШТЙСЬИЙУЙЮУМСЖЦКЙЙМЧЦЧН
ДЩФЫШМАЛСДУЮФХЮЙАЖМНООСМЮ
УБЧЦЧСУФХБСЫЛНДЖЯЛФПВЪЙПП
ЖЫЛПЪИЦТЯБИОСМЛТЖСМЛТТСТС
РЬШАЫРЦЭЙМСЬПУБЫОСМЙЙЫЖХО
СЬЙТИМЮЖСБЛТЛЬЙМУЙТНЦКОМН
ООШАНЙПЛРБХАЖСЬЦЦЫТИУЬЙТН
ЦУЖПДЪОИИККТЛЖНЙСЦЧНЦЫЛНД

ЦБТДЙСУПЖЛЙЕЖПШМШФЫБЖКЛЖН
МЮФЦНЦРФХЖМАЖСДНЭФСПФЬДЪБ
УКДЧСТТЕЦЭЙХНЖПООСМФАШЖЦЫ
ЦЯЕХЗЙХБЦЬОЭСДУЙАЦДГПБРДО
ТЩВЙОИЬМИШТЯЛСЙМЧНЖБСЦШРК
СЬШТЙСЬЧЦБОЩЕСЙЯУИХСПЦХЯН
ЦУРПЫСЫБЙНЦЬУЯДЦНУЙОХНХПЬ
ЫЦЩЦСЫЦКЛЗКСУЭЙИДЯШЙЖПОЧПБ
ЛНШХЫМЭСДУЕУЧОКСУЭЙЙМЯЩРМД
ШЧТУМАЧГНЖЦУЪКЖЬОХКСЫФЛЮЙ
ЫОЦАТФКАКХУУСДНХИЙЙМАТТЙТ
АФСЙТШФЗКЦЬЩЦМДАОПЫЖЫФЫШБ
АЩЛЗЧМРТЯТШШТОТБТЙМУЬРТИГ
АФХЖЧМУТЖЦЬИХЛТЪОСЬВНЧСКЖ
ООХЙТРЖОКЗЬЧЩКФЬУМЗГШФЗКЦ
ЬЦТАСЬЙТАДЖСТЖТЪУЙНЫОЧЦШЙ
ЫФХЯМЫЩПКЖЭФПБПМЗМЗРУУГЖЦ
ЬШТЙЙРБЦБФЭЛПЭТЩОУКСНИЬДЫ
АФМНОЮЩЖИЙЫЕСБЛОЦТЙМАЩЗЬХ
ЯОФКЦООЫПКЦЛЩКФЬУГОДСКЙОТ
ЭФКЬФЬТХЛДЩОПКПОЭЧЯМЦКЙОМ
ЯЙТМЙЩООЬОЭСДУЧАИТЖФБЙЙОТ
ЩВЙОИЬМИШТЯЛСЙМЧНЖБСЦШРКС
ЬШТЙСЬЧЦБОЩЕСЙЯУИХСПЦХЯНЦ
УРПЫСЫБЙНЦЬУЯДЦНУЙОХНХПЬЫ
ЦЩСЫЦКЛЗКСУЭЙИДЯШЙЖПОЧПБЛ

НШХЫМЭСДУЕУЧОКСУЭЙЙМЯЩРМД
ШЧТУМАЧГНЖЦУЪКЖЬОХКСЫФЛЮЙ
ЫОЦАТФКАКХУУСДНХИЙЙМАТТЙТ
АФСЙТЖЛПАЙЪФСПЗЮДРЧНШУЙГИ
УЮСДРЭЦЙАЙЩЖРДХТЛПЬПЪФННД
ТХЧНЦЙЦЙИУЬЙТМЙЩБРКЕБЙПДЖ
ТЛФБЖКЕУКЕЮЛПЛТАЦТЛМЫРЙДУ
УХПКРХЖХЧУОСКДЖЙЛЕЬФРОСЖМ
ЦЗФКХЦИСЬЗЮЕИЧУЬРДИЙЫУТЕЗ
ЮЩИБХЪЛФОЙЩВСКНАЦЙЮТСФНГД
ЯЛГЗЕУНПЪИКЛМНДЪЦДНЦЮЛЖКК
УУСЧНРЙЧХЧПЩФШГЫЖСДЫШФРЛТ
РЖПДПЯЕЛЮЙЫЕТЗТРЕСЙТЦНДИЙ
ЮУДЖДЪУЙУЦЬЗЖЧУЩЖОЬЦКТЧУД
ЯВЛЬУУРЬДЩЯЕХЗЙХХТЖДНУСПВ
ФЙЧУЙЯШАОТЩВЙОИЬМИШТЯЛСЙМ
ЧНЖБСЦШРКСЬШТЙСЬЧЦБОЩЕСЙЯ
УИХСПЦХЯНЦУРПЫСЫБЙНЦЬУЯДЦ
НУЙОХНХПЬЫЦЩСЫЦКЛЗКСУЭЙИД
ЯШЙЖПОЧПБЛНШХЫМЭСДУЕУЧОКС
УЭЙЙМЯЩРМДШЧТУМАЧГНЖЦУЪКЖ
ЬОХКСЫФЛЮЙЫОЦАТФКАКХУУСДН
ХИЙЙМАТТЙТАФСЙТЩЛТЛТЩВИНЦ
ОЪШКХУУСДНТФКАА

9) *РХЮЯЮАКШВЬЯБЛОЙЩПЪСОСРИГША*

ЕКСОТТФОЫЛЪЬЖШФУОЖЮШЗДЙЯМ
ЧСШУЭБКНОВХЪТЬТДЭГЬШЪОЕРР
ЦГЖАРХМТАХХЛМТЫДЦСОБТЪЛЬЦ
НБТАРЗДЙУЬНДЖЫМГЪОЦГЦЩФЩШС
СЗШАНЦМЦТАБТШРРЛЙГЭКЯВУА
КПЙХХРСОПЛРФСЬСУЦООТУЧПШР
ЪУБШРЧЪРЬЫУЭОБЫЗЦСЬТНАМОЬ
ЕЩЕЯЪУСИУАТЪЛЬЫУЩЙОЫБЩЬЧЕ
РЪРЬЪНЬЖШШФЪГУЫКЧЙЪЭКЫМЙТ
НШЙЫГЗДЖМЧНШПЧЯШЭУЬЩПМЛЪЮ
МПНЩРЙСОДРФЪЕЫХШШПЩЗТЗКРЮ
ОЫСЦЫНОПРШЗСУЮЮЗНЖФРРЛГЙЪ
НЩФРЯУНЖТЭУСЛЬЫКЩЧУТЙЪМКЯ
УНЖЮХЛФКЭЮРЯПЯВХЪГЬТСЪЖЮЮ
ЛРЖЫМКПСЬЬАОПХТКЭУЦЫНФМУУ
ЬСРЮЮЖЦЙЫРЪЬЖПВКШПЮХОЫМНБ
ЕЧАТХЦЛУКБШЮПШСКУФЯШРФКЦУ
РЯРЬУУРПСЫДРБВЮТМСУЩТСЗЫХ
ОМОЦБЕЩБХГЖМЦЪРРИШЦИПФЖЩЮ
ЗЯЯЪЮГЭЛЬАРЯРШГЗСТУЫДЪУЭП
ЧСОЯШТФЦРШТФГЙБУБЩУЩЮЮСЙЦ
ПФГЬФЕЪНЙЫЕГСУТУЦПЮРЖЧАЭЮ
ВШПЧЬРСШЫЮЦЮЙРФХЯДЬСКЬОБЫ
ЦЛЦОЮЦШЖЮЖЕКЪБОНУЛЬЭЫМГШЮ
ТСЧНЯУЭУЦУЕЧМОЧШЬЭРЪУЮПЮЮ
ОЦПЩЛЪМАЯМЗЭРЩЛЗМЖАЧЕГБЮЮ

ЗМОЫЛОШЖЮВЗСЧЬСЯЛУЙЩЦФОУТ
УХДЬАЬМКЖХИЪВУЧШШЭНТУДЖТИ
КППРЬУФНУФРФУУЫБЩЬУБТЗРЮШ
ИЯВЦЫДФИШГЖЦБЭХХОПЩГТИАПА
УТЖЫШКЧЯПЮЗЩПЧААТЙЫЛФЪИЫР
РЛТААУХОУСКЭЙЪХХЯЙГУРЯВЦЭ
ЕШВУБЦЮСОБЧИЖАХЦЩЬГЭКРСЯВ
ХСНЫШТРЖРПЧЗКРРРШЖЮЖЕКЪЦЩ
ХМТЯТКЮООФЖЬЙХЮСППЩГЖФОЙЬ
НЮПЬЗКШРЮШЛФИЫШТСНУЗЧММХР
ПМУЩШРЪГЙЩЧЬЖЭХЧММЫРЙЭУОФ
УШГОЫУОУРХХРЖМЙНБРЬТКГЖЮР
СФЦЭГХЫФЮСАЧТЮЮЙЩЙЪШЦЮЙЕХ
ЦЦЙЪЭЕЬАТРСУБРХЮМОЫЛСМЛАХ
ХМНТАКООЦЕЙЬБЪЬТСДЮХМФМЦБ
БЭОУУЕЪДЫХОУЖЩХТЗЦЯВХЯОЙЭ
УГОЬЩПЬФСЮЗЪСЬВТСТЩЛЪМОЫЛ
ЪУБЮЭНВЙЩГЬВЖЩГГЕЙЧУРМИОЫ
ЕПФЫЛНЫСЬСШТЕУЭБСЗУЫЧЪТЦЭ
НБРАШЫЫПШГЙМИЙСНЮПЭЗШЮРЬС
КЬЖФМКЦБШБЧМЕЬТКЫСУЩФЬФЗШ
ЪЩБАРХМОЫХЗСЕОПЬЮПЭПЧЦПЧФ
КОЬПЛРЫПРХХТЖЫШШЭНЦАКЩБЯВ
СМУЦЪУЦЖОЭДЯДЩГЖЧАЩБДОЗСГ
ЬЯЯВЫУЬЙТГИРЖРЫЕТОЙЕИЧБХЯ
ЕЩУУАБФМУЯКЭУШШЦЬПТЭНЧЙЯМ

ЦАББЭУХБЫВХЪРЬЬУЬХЫЮООЭГЦФ
ШФПААЕТЖЫМДЬБТГИЮБШЫКПЛЦХ
ЮСАЭЮЗЭУЮХЬММАРПФЖЯВХМОЙУ
ЙСГАААУЭУЫШПМЦПЫШТЕООЮФЦПЮ
РЪУЫХЗССЬПЧЩЬУУТФЯАЫКОЙОД
ЕЩЬЫРЦЮСОЦКМЕЬТАБГЬАУЮРЬФ
ФССЩРСЯУЮЮЗЗНЦЫКРОЦЪЕШЙРФ
УЧЭЬВССМУЩММНШЭШОЩЦЕЗБПТТ
ММЦТРФБЫЛЬССЫЛЪУНУЩНУЫУФ
КЩОЙЕПЧПЭРСФТРШЦМЯАСШЬЖРР
РУМЬТУЩЙУЬУНГЦТФЪЯЗШЪЬЬПЮ
ПУПЩЮЧЗЦНТЦЮСУВНЧГЬВЖЗРЬА
ЕРПРРРМТКАКНАЭДЩЖРХЦЮЭЬВ
ПЯЕОЭЕЧЖАХЗДЙЧТКЮЖЮЪНЫЖЫМ
КШМУЯКЭУШЮЗЦСЬЯНЧНУЭДЯУЬЬ
РСООБЗЪЙЪШФЪММБЕШЙЭГЬФООШ
МЬБХТКЬТАЮОПМБСНЩЬРЧЙЗНОП
ИЬФТМЦЧЙЪЮТЩЬЪШЦЪТДРСФВОО
ПММОЬКЩАЭЮЙЭУЬЭЗЪМЫЛУПЕОБ
РСУОЫЕНЖЩЮИЧБХЛЪГБУЪЦЮБНП
ТМТУСКЦБЕРРФЦЮГИМОКШФЪНУВ
ФЪЕЕРЦШПЧЗШЮЛЦЩЦЪОЭХХСТУЪ
ЕЛФАЮФЧЖЫЭНЦТШЮРИИЦЫЦЫЙЫЮ
ООРУАКРГШГЙЬАРЛЪПБРРТЛЦСФ
КОЬХАКОБМВИМИЙЯБЛОНЙНБГЬФ
ДНЬЩБЕШЙЪБУНПЧЭННСЬЭКЦБАХ

ХМОЦЯЕЬФЯЭНЦЙСРТУЬЫХЦЮСЬЭ
ШЧЙПЛЦШЖЯВЕЪТАЮЗШПЧ

10) *ШЯИСЬРГУЮЖУВЕЩКБТНЦНАУЕЪ*
ЬЮЯЙРКЯГКЦЙУЭКГЖЦЖЛСЬЩЩЙАС
ЯДХЫЮЙЪЗХГОЮЧХЕЯГЗНКАБШЮН
ШЯОГБЮЫЗХКАЬКЯЬЩЫУРАОАХХЙ
УУЦЧЬНВЧЫЗЦЗЕФЬПМЗПБЩЩЬХБ
ЯУУТЖОЫУЬШНЮКПФОРЖШПТЮНГЬ
ЫЦМЪЬЩСПЯКПЦХТОУЦСЪБСЯРЫН
ПМРЫЙХУЕШПАЦЭЪКЬЮИЫЮЬБНШДТ
ЩЦЛАОЯЦЯЬРНЦПКЧЫХНЕСЬШВКЧЩ
ИЭБЖЮАЦКЯГЕПШЮЯЦЮДМЮЕПНУФ
ЙНЫШБУПШЬГХАЖАУУХСЬГСЫЪЦШЦ
ТМТЗЕПЧЫДЬТМЫМОЮОЙХДЪКРМС
ХИУЮКЩЛЬЫХЫЪПЯРЙЛЬБЕУБЫЩОХ
КПЩЙЪКЮСЗЪКТДЭЪКЦВФЫЖЬЪТЫ
МБЫЕЩДНШЕЩЖЫДРННЩДЪДОЬТВЯК
ЧБКДШМЮКСКЯГУЦЙЬЪТТКЯЫЗТМ
ЫЩРЮЫЯЫУЭЭЫМОСПГСТЪЬОЖСНОЬ
УЕДБЮЮКТОТЯХЫЯОАХХИЬБЦЧКС
ЯЦНАОЧКШОЙЩЦПБФЩЩЫЙОБНМКЕЦ
ТЙНЭЯПЫЕЫСДЯКЩНПЫЙУЮЕСКЯЯ
СЪКМЯТТИСЯЗЫМЦГБЯЧЪЩРИЕЦУК
ЭЙЙЪСИЭБХКЩАЮДМЙЫЪЩИАЗНГБ
ГБЩЯЗНОКВДЮООБКЯШЦЬКРЖЦЦСТ

ННЗАОПТДЧЪЬТЮЕЩДШСПЮЙУЧТИ
БХУКФАЙЬКЯБАНЕЪЙОСЪЩЬАЯЗНК
ТЮЕХГЭЦЦТЙШЯЧЫМЙЦНЮЛЬЬТМЗР
ЦХЯДЫВПХЕ

11) *ЦИЪМФЧЦФОПЫЦТЕЧМОФЕШЭКШД*
ЖЩДПСРМТЮЙУФЙГДВЬИЧВЦМЪЭИЬ
ССЫУРМКЮЙОЧДФУЦЪСШМФНФРНЩЮ
ЦЩТЖЦЗТЕЧИМХНВШРЭУШЗОФАСЦЦ
УДЖЭЦЩДЩОЧЮДИМУЬОПЮИЩНБХТТ
ЕЦЩГЬСЩЩМГКЖШЩЗАЧЮУШВБХМХН
ВШЦУУЧСЛЮДУЛЗТШЛЭЪЮЙЧЯХФУРО
ЩГНКЯТХЩЛЩНЯОСЩГЩГФЬЩВЬНЪУЮ
ТЖЩИЪОХЧНЭНФПЦТСБЫИВЬУСФЭОЙ
ЪТРЖЛЮЩПНФЫЦЭЕТЩЦУУЧЪТАОИФБ
РРЖЭЪГТЭФЪРЛЕПМХТФГЪЮЦЖЬДЮД
УМОФЫИЪРЭАТЭКЮИТОНЫЕСЭХХСШФ
ПХМСФЧЮГФЬЩВИИЦЫЗУОПЦАДБХЭЮ
ЛТОЦЧВБЭРЫСЕФЮРРВШЦУСИЗАШНБ
ЭКХСЛЧДХМФУРААШИРФОСЫЦЪРБЮГ
ЩБЛЧГЬИЮМЪААТФРЬОЦСЛФЕЗСОРЛ
ОЦЦААЗЧРВАРЛЧЮГФЬЩВИЗСМЭОПЫ
ШШНФЭЗЯРООГЗНЩРИЭЬТЪЖБЮКМКЯ
ОКОИЫВФУХХСТЪСЕОСШРБВБЭЦВЫЛ
ПЦЬОЙЯКЧИЦМЪМНЖОЩХЧШЪФЭЕХЪМ
ТЛЖЭЪЭО

12) *УЙЬГЬВЕЗГТОУИЯООТЧГОЮТЯФЕЬ*
ЦЙУЕУРХЦНЗЦЕЭОЩЬЧЬООТЧХИСЖЬ
ВЕПЕДАВЪЙТФНФЪДЧБСЦДАИУШГВУ
РТТЪШСРБГНСИЕФБСРЬЧЧССИЯЕПЕ
ЩКЕЧПЧЗПСЦБАВЧНПОСФМТЧПЪРТЯ
ИЬЕИДИЮЕВЭАБЙВСКЪЬЬФЫБУЙТРФ
ТЬУЕЭЕЮЦЕЭБДЧСЦЕЮТНЩУИЪНФНИ
АЛЩЫЬФИБПЧЬАРЦБЪЙЪИЕЯЬЭЕБТР
ФЗЮЯОХТТЫЧМЦБАГРЕГЪРМЛЮЧРЦЕ
ВОНЗОИАЛИКЙФЕЭБГЪРОУЫЪНОКВЪ
КФОИАНОЖЬЩБЬКЭЯЫХЖВЧСЦМЧХРМ
ТУЩЕШРЯБЕГЕВОНЪОЩГАРАЫШИЩТЧ
ДУЩУИЪТРШПЕОЩЕЙТМЮКОЧТЮЕГЭЬ
СЧИСЗМЧКЮАЩУГВЕЦЕЩГЕБХЬЬЛММ
КВНМДБАВЭКЗОИОЦЬЫЗССВЧВЭКГБ
ЛССЬЯАШНИДРМТЧЮСЯРЯДПЪПЕЫТС
ХЖЪМЪРЯГЬФЗЬВЬЫШЙЯИЦТЬУОХЦЦ
ФПЯЦЙННСЬКЦЕЭТЕХОШТЕХОЙЧЕЯЕ
ОНМВИМЙЭЪНЩАЙВЕОУЭТТСКФДОМХ
МТНПКВГЛЯИЧЮИЧУИЧРРТЕХОНУЪТ
ВРКГАНЪЗДАЧФСЬДНЯРЮАЛЪЧЕЧКЪ
ФУЧОЩТЧЬЛФТЕЬДЪЪДЕЛФЛЧЭОСИЕ
ГИЬНАГКЪИЕЬИЩЛЧЭАЫУГЧРЦРЕФД
ЗСБЧГЪРКУОХФЕЦДЗСБАЙЛХОЧЗМЖ
ВЪСЮЕВЪУУУЗНЗЪРЕДАЩЕИДАЧНИФ
ОСООЧРОУДЯОКХЬЩЬНУАФОФСЦУОП

ЕЯБРЪХЕЬАЫХЕЙТФЦВЕГМТЬУЕЭНЗ
АКМЦЩАЙНХЧЯНЗОБЭИГЦБТЖФПЧЬИ
ШЙЬФИУУГДВЪОБЭИЩУБЕКЬЕПЧНФУ
ДГКММЧЭДСЗЯЩМЪОИДРМЭЬЯОЩЧЧЫ
НМЧЧЫНЙРЯЖЛМСГЪМЙРЯЖЛМСГЪМЩ
УФДИУТЧЬИЮКГЯЫЦЕББУЮБЩЩАПХЕ
УНЪСГВАЦКИАКЬАВЪХЮЕАЯУШУМТМ
ШКЫЮОЧЬЯЮОЧЬЯГКММЧЭОЩЦЙВОПУ
ДЧТОСЯВЕНУЪТКЬУГЧБЪИЧГИЧБДЧ
ЕЮЕАЯЫЭНВННСЧИЬАУЕВЬОЭТКЭСЛ
ДЙТГМТЕЮЧСРЧБОРЭЬЭКЪЗТЮТКХШ
ТНЪСЕЬИЩШВШАЬПЯЫАЮСЬЫДМТВЧН
ФЗТЮВУИВСДЪСМЪЩЩУАБТФЫТЪТФЪ
ЕГИЩНЬВЕЭТЯИЫЪФЦДЬЭПВАНФРДТ
ЯЮЕЪТН

13) *ОШЫДВСРАХЧСОБФТСТСЫСЛЙПЕ*
ЯРНБЫЛНЛНЙРОРОЮТНЧЦЗЕХШЕКЧР
ДАЫПОЕФХЦОЛТГОШЭОСЫЫЙОШЭАВО
ЬЕРОСОМЦЫЙССМЛОЦНСТЧШЕНЧДАС
ЦНСТЙШИТДАШЛЙХЗДЧЩАЯКЭОССШВ
НЧДЬЗЙПЕТЦЫЕКЧШЬЦЧЯЫОЫСАЛЙЮ
ВОЗЮУДЕОУДЩАГОХАИЯРНБЫФЬРЕУ
ЭАСЦЫЕЛСГОТИЪУЛСЮЬДЦХМОСЬРО
УШЯТДЩРООЩВИЦЫИСЫЭАСЫЙТЕЩФА
ЛСУИЗЦЙМОЗХВСШЫМНСШЯТООЯПЩТ

ДАЦНЛООЩИЗЛНЛТООЯКЙЧМОФЫДОЪ
ЯЬСЛЫЮЯРПАЛЫТБЯЦЫТЫЦТОГФМНУ
ФНСЬИЮЛЕРИЛИФЪОТДЪЕСЦХЗОБША
ТДПСИЦХЙПФНЩСШЫКОТЪОЗЙПЕРЦА
ЛАЪЙВСДЭУЮЦЫЧЬЫИИЗНЫМУЬЕЛАЬ
УНЕХТЧТЙЯЬОШЫДВСРАХЧЮЛАЛТВС
ОЩИНЧПАЛЧЮЬМЧШОДЧЮТЬШЭОШФНТ
ВЧТЛИЯЫВЕМЫПРЧЮТОТЫПРЙПЕСЛЫ
ЕЙЩАКОТАБРЙШЯСЧЮТОФНАЛОЧСАЦ
СРБФЫК

14) *БРЖГЯРЮРЩТОЕЗШЕТЯЛЧЦЦЬЕТДЩЙЗ*
ЩЭКГЮЬБИЯЖХВХЦОРРПЫПЗНЯЗФШЬ
ВЫЩЛСЖЩМСЙНАЪЩШНЮЭКНИХЮДЦХЩ
ЛЯМРМСЯЩДЮАПУШХЫОЗУСИМЖЖВФЩ
ЫЕЙЩЫЕЙЩЫАФМРВИЯУВГЩГЬТЯЛМИБ
ЗУФЖЩМСУЮТУФВЕРБЛЯФЦРЖИЕЭЬДЗ
ФСХЦЩГОФТИТВЦОЕВПЬИЛЮВФЖНЯХ
ЩЪЕУРЬКЦГРЕФЖЛЛЕЪРЛГБУЯШХЖЛ
ЯАЩЯЛЯЗТЮГЫИФБУЛГЕЗМРЩМУЗЖЩ
ЯЕЩЬЕРБРЙЖЗЦКСЭЫАРРЙПУВЬКГЮЛ
ЛРФЫОКВНОПЮЩНИЦЬЕППНСИАЖВАЖЩ
МПЬЫЕХЯРНРПЭИШВЦЬИЖЬЯФХРЛЮЙ
КБОВШЬПЩПЬДЗПЬЙЩЭЫРФНЕНХЦАЖВ
ЬЛСЦРНРВВТСГЫИЫЯЩПУВБВИЕЭЬЛЗ
ЧЕУЩЭЬФЩЫГИЭРСИБУН

15) *ШТМЦАЩАОНЯШАЛФОУКЮСАМЦХЭЕХ*
ЯВГФШЕУКЧСАТКЬЦЗОКЭУЯПУСЭНФП
ЕЪАНБУЬЫПКЯОВХЭЕЬБРПАЧЮРОЮЫА
ЕУЯУЦЗРЧЫЬРИЦОЬРТЙЦКЮЦЬОШКТЧ
ЭЧЩЕЭКЯРЬДЬЦХЭЪЪАЗОЯУДПЕГРЧФ
КСЭАЛЙЕТАТУХЬЫПКЦОЭЮТЧЧБРЦЮЬ
ДТКДКЬВПЪСВВГДТЧФНЯОЬХЦДОЗЙЕ
ИРЧФЕЧАЬТАШЬФПНЬЦФЗМЕАЬКХБЦЙ
КМТЬХТЕЦЬЫМЧААНГХТАЮРОЪЩЪНГУ
ЬФПНЬНЯЗФАЪЯАНБЬЮПНДКЯЗТТТАМ
ЕЬЯФЗЧЭЬЩЖКГКЪМЕЬПЧУФВЦРФТАЬ
ДЖАЗОЧФШГАТНУЧАЧНУТЭВРЪАФЪЗЙ
ЕЪТАЧГЪЕФТАРЧТТАААНБЬЬФЩКВОА
ДЙАРЧНЕТЫЯВЕЗЪТФУФОССБРХТТЕЩ
ЬВЗТЯЙЫЖУЮХТЙРЕМШКМЯКЮРГЩОАЖ
НЯЬЙЗЦДРАДЙФЬЧОНЩОДЗЖСНБЮГЩО
ЭРЛОЪЧПДБЮЧЖЕФЖЪЧИЕПЩВСЧЮДДА
ЫГАНУЦСЭВМЩОДРЬДЬЮКХШУГФУЬЦХ
ТШУХТФУЙААГУХЫЧУФТЯТПТТОЗОЕД
ЬФВПАСЦВДЯЬЙЮГШТЕЗКБЮЪЧУЦОШК
МЯКЬВЛЧАГБЗЪЯЪФТТРАНУГШЧЩЧАЭ
АЩКГАЪЩЧАМЯРЦДКЙФУГРАГУЦОБТК
ЦЪЪНУЫСАУЧОУЫУЙЕТАЩПАЧФТШЬУЪ
ДУДРАЪРТЬДМНЯБФСУЬЮНДЕЭЬФПНЮ
ОДЗРОЫАДМХЩСПШЭОЯВСЧЫСЗОХЬФР
ХРАННБЦОЯФШЦЦЬФУФОЭВЦДЮТПНИЙ

ТЖЕААФЗЬТУДБЕЯЫТВЪЮОДРЗТЪЕЙЕ

16) *ЖБШЖТТБУГВАИЦЯГГЖФОРДЧШППХАС*
УАУЕИЛАИЦШХЮЬХЧОГЬШРГВУНБВБВ
ХЭБНДЪВУТБЕГГУУПРРГСИШЮФГПД
ОВСБЕМОЭЛХЪЖФХВХЦФХФИСЪБПЕГ
ЧЦЫШЭСЗФУЕЯББНТЧХЦЫРЮСФУУРЖ
БЕГФШАРТЩЙИФЪХЛСРЛИНПДОЧИУО
МЧУФПГЛЛЖРЮФГБЮИЛЛАИЖЮЮЯСЛШЛ
ХЫУЗОШШХЙЪЮЛТВХИФУТУДЭБТФРЪЗ
СЛШКДСУЕЯЭУЦОШКЦКФОИРГЪЮОХФ
ЮПШВСХВООЯЬАИЧЯГВРЮЫРДФЯИСЭ
БСЦЭЫШТВГИОБТВМЯГИИРЮФГЮЧРТ
ЩЯЦЛЛЭИЦАЖЗЙЭВИФТОМЬРЦЛХЪЖЪ
ЙЭВИФТОМУГЕЯУАШСИЮЮИППГГСЭЫ
ИСХХКЗЮЧЮФХЯИХЫБТТБЕГЖШЮВУЮ
ЧРТЦЫИРШДНЧБДХЖГТФИХЮГПБТУЙ
ЬШФПХАРМЪВИФБЕГРЯГЛИРЮТТБЮЦ
ЬЭЖБХГИЦВСШЖПЮДХАШХУСЮДХАГИ
ЦЛТЖНМГЯИФВХЛЖЬЖКЯЪЖВФРЪЭГЫ
ЭГОВГЦУЯБЕЙАЫОГРЮЖЙСГСНУУУР
ЮАЛВ

5. Модели систем шифрования

Задача 26. Пусть $M = C = \mathbf{Z}_n^t$ $(n, t \geq 2)$ – пространства исходных текстов и шифровок соответственно; $K = \mathbf{Z}_n^l$ $(l \geq 2)$ – пространство ключей. Считаем, что вероятности на всех этих пространствах распределены равномерно. В качестве системы шифрования используется система Виженера.

1. Доказать, что при $l \leq t-1$ такая система не будет совершенной.

2. Что можно сказать о ней, если $t \leq l$?

Задача 27. Пусть случайная величина Q принимает не более t значений. Чему равны минимальное и максимальное значения энтропии $H(Q)$ при всех возможных распределениях Q?

Задача 28. Пусть X, Y – случайные величины. Справедлива ли оценка

$$H(X|Y) \leq H(X)?$$

Что можно сказать об этой оценке, если величины X, Y независимые?

Задача 29. Верно ли, что для любого шифра справеливо равенство

$$H(M|K,C) = 0?$$

Тот же вопрос для соотношения

$$H(K|M) = H(K) + H(M).$$

Задача 30. Пусть E_1 — шифрование шифров Виженера с длиной ключа 12, а E_2 — шифрование шифром Виженера с длиной ключа 22. Что можно сказать о двукратном шифровании E_1E_2?

Задача 31. Пусть E_1 — шифрование шифров Виженера с длиной ключа 18, а E_2 — шифрование шифром Виженера с длиной ключа 39. Что можно сказать о двукратном шифровании E_1E_2?

6. Простейшие шифры

Задача 32. Выбрать язык (алфавит), матрицу шифрования шифром Хилла размера не менее чем 3 на 3 и зашифровать фразу *Моя фамилия...* (можно выбрать другую фразу или использовать другой язык).

Задача 33. Построить шифр Виженера с длиной ключа не менее чем 5, выбрать фразу длины не менее чем 50 знаков, оцифровать ее и зашифровать, используя построенный шифр. Привести вычисления длины ключа, использующие тест Казисского (т. е. вычислить значения функции Казисского для прореженных текстов). Соответствуют ли вычисления теории?

Задача 34. Доказать, что кратное выполнение шифра замены для различных ключей $\sigma_1, \sigma_2 \in \mathbf{S}_n$ (n – мощность алфавита) равносильно однократному шифру замены.

Задача 35. Что можно сказать о композиции двух шифров перестановки с ключами $\tau_1 \in \mathbf{S}_m, \tau_2 \in \mathbf{S}_k$?

Задача 36. Доказать, что композиция двух шифров Виженера E_{k_1}, E_{k_2} с ключами k_1, k_2 длины l_1, l_2 соответственно снова является шифром Виженера E_{k_3} с ключом k_3. Чему равна длина l_3 ключа k_3?

Задача 37. ШИФРОГРАММА № 1:

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

Известно, что эта шифрограмма получена шифром Виженера. Алфавит английский – 26 букв, занумерованных от 0 до 25. Длина ключа неизвестна.

1) Вычислить длину ключа. 2) Найти ключ. 3) Найти зашифрованный текст.

Задача 38. ШИФРОГРАММА № 2:

Щ Ц Ы Ж К Ч У Ц Ь С Д Ъ А Ц Б Т И Т К Ф
Ь Л Г Ъ Ь С Ю П Й Э Х Ч Р Х К Ф Ш П Н Т
А Э М Н Ю С Н Я Ц Ч П К Ы Ш Х Н Р Х Л Я
Л Ч Ч Ц О П О Д Ъ С О Х Й Щ Е Л З Л Л Ф
Ц Ш Т Л Ц С Б О О Ь Ё Р Ь Т О Ю К С Я Щ
А Ч У Ъ П Х Е Х В Н Ю И Л Р Ш Ц Ь Е Р Р
Т Е О Х Й Н Щ С Ъ Ё Б Ъ Н И Ц Ц Р Ъ Ы Ч
Ш Ж С Ц К П Ц Ш Л Я Н И Д Ж Р К У Щ Ь С
А Э М Ч Ч С Р Л Ш Ц И Р К Ч У А Я С А Т
У У Н С И Ш О Н П П З Ъ Ч Ы П Х Й Ц Ц С
Ы Х К Я Х Щ Н Я Е Щ У Ч Ы Ш К Л Т И Щ К

Е Н У Р Ъ Х Й Э Э Щ Н Я Е Щ Щ Ц А Ж Й Щ
К Ы Н Р Н И Щ С В Т А Ш Ч С Ъ

Известно, что эта шифрограмма получена шифром Виженера. Алфавит русский – 33 буквы, занумерованные от 0 до 32. Длина ключа неизвестна.

1) Вычислить длину ключа. 2) Найти ключ. 3) Найти зашифрованный текст.

Задача 39. Для какого языка индекс косовпадения абсолютно бессмысленного текста больше: для русского, английского или армянского? От чего зависит величина стандартного индекса косовпадения при одинаковом количестве букв в языках?

Задача 40. Пусть задан алфавит из n букв, занумерованных обычным образом. На платформе $\mathbb{Z}_n$ определен шифр, ключом которого является вычет $k \in \mathbb{Z}_n$. Шифрование осуществляется по правилу:

$$E_k : m \to k - m(\mathrm{mod} n)$$

.

Показать, что этот шифр на самом деле является аффинным.

Задача 41. Имеется достаточно длинный литературный текст английского языка, использующий

только 26 букв (удалены пробелы и прочие знаки). Текст зашифрован методом простой замены. Взломщику разрешается узнать кодировку любой буквы по его выбору. Как он сможет узнать кодировку сразу двух групп?

7. Группы

Задача 42. Сколько решений имеет уравнение вида $x^2 = b$ в группе $\mathbf{Z}_{21}^*$? Привести все возможные случаи.

Задача 43. Будет ли циклической мультипликативная группа $\mathbf{Z}_{24}^*$?

Задача 44. Сколько порождающих элементов в мультипликативной группе $\mathbf{Z}_{23}^*$?

Задача 45. Доказать, что абелева группа порядка pq, где p, q – различные простые числа, обязательно циклическая. Верно ли это утверждение в случае абелевой группы порядка p^2(p – простое)? Построить пример неабелевой (заведомо нециклической) группы порядка pq, где p, q – также различные простые числа.

Задача 46. Доказать, что в циклической группе $C(p)$ простого порядка p любой неединичный элемент является порождающим. Сколько порождающих элементов в циклической группе $C(p^2)$ порядка p^2?

8. Конечные поля

Задача 47. Построить конечные поля $\mathbf{F}_{2^4}, \mathbf{F}_{3^3}$ и $\mathbf{F}_{5^2}$, указав соответствующие многочлены $f(x)$. Найти порождающие элементы мультипликативных групп построенных полей. Будет ли элемент x (в каждом случае свой) порождать мультипликативную группу?

Задача 48. Доказать, что в любом поле $\mathbf{F}_{p^k}$ содержится единственный (тривиальный) корень p-й степени из 1.

Задача 49. Пусть поле $\mathbf{F}_{2^4}$ построено по многочлену $f(x) = x^4 + x^3 + 1 \in \mathbf{Z}_2[x]$.

Перечислить все элементы $a \in \mathbf{F}_{2^4}$, для которых разрешимо уравнение $y^3 = a$.

Задача 50. Доказать, что в поле $\mathbf{F}_{2^6}$ для любого $a \in \mathbf{F}_{2^6}$ разрешимо уравнение $y^5 = a$.

Задача 51. Перечислить все корни из 1 степени 4 в мультипликативной группе конечного поля порядка 27, заданного многочленом $f(x) = x^3 + 2x + 2 \in \mathbb{Z}_3[x]$.

Задача 52. Пусть поле F_{2^4} построено по многочлену $f(x) = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$.

Перечислить все элементы a данного поля, для которых разрешимо уравнение $y^3 = a$.

Задача 53. Сколько решений уравнения $x^p = 1$ имеется в простом конечном поле $\mathbb{Z}_p$?

9. Дискретный логарифм

Задача 54. Вычислить методом Сильвера – Полига – Хеллмана дискретный логарифм элемента 25 в поле $\mathbf{F}_{41}$ относительно порождающего элемента $g = 7$.

Задача 55. Построить поле $\mathbf{F}_{7^3}$. Найти порождающий элемент g его мультипликативной группы $\mathbf{F}_{7^3}^*$. Вычислить дискретный логарифм $log_g f$ по основанию g элемента $f = 5x^2 + 2x + 6$ методом Сильвера – Полига – Хеллмана.

Задача 56. Построить поле $\mathbf{F}_{3^3}$. Найти порождающий элемент g его мультипликативной группы $\mathbf{F}_{3^3}^*$. Вычислить дискретный логарифм $log_g f$ по основанию g элемента $f = x^2 + 2x + 2$ методом Сильвера – Полига – Хеллмана.

Задача 57. Построить поле $\mathbf{F}_{3^4}$. Найти порождающий элемент g его мультипликативной группы $\mathbf{F}_{3^4}^*$. Вычислить дискретный логарифм $log_g f$ по основанию g элемента $f = x^3 + 2x^2 + 2x + 2$ методом Сильвера – Полига – Хеллмана.

Задача 58. Построить поле $\mathbf{F}_{43}$. Найти порождающий элемент g его мультипликативной группы $\mathbf{F}_{43}^*$. Вычислить дискретный логарифм $log_g f$ по основанию

g элемента $f = 11$ методом Сильвера – Полига – Хеллмана.

Задача 59. Продемонстрировать версию алгоритма Сильвера – Полига – Хеллмана вычисления дискретного логарифма в поле $\mathbf{F}_{17}$ для случая $3^x = 15(mod 17)$.

Задача 60. Построить конкретный протокол Диффи – Хеллмана с платформой $\mathbf{F}_{27}^*$.

Задача 61. Пусть дано простое конечное поле $\mathbf{Z_{43}}$. Предположим, что g – порождающий элемент его мультипликативной группы. Сколько всего имеется порождающих элементов и как их можно получить из g?

Задача 62. Предлагается следующее упрощение протокола Масси-Омуры. При выбранном конечном поле F Алиса осуществляет передачу сообщения $m \in F$ Бобу. Она выбирает секретный элемент $a \in F^*$ и передает элемент ma. Боб выбирает секретный элемент $b \in F^*$ и передает элемент mab. Алиса умножает на a^{-1} и передает mb. Боб вычисляет m, умножая полученное сообщение на b^{-1}. Какова основная слабость протокола? Можно ли его улучшить, заменив платформу F на кольцо вычетов $\mathbf{Z}_n$?

Задача 63. Пусть дано простое конечное поле $\mathbb{Z}_{47}$. Предположим, что g — порождающий элемент его мультипликативной группы. Сколько всего имеется порождающих элементов и как их можно получить из g?

Задача 64. Предположим, что используется система Меркля-Хеллмана моф, где p — простое число, равное 2503. Шифрованный текст есть $c = 3155$. Вектор открытых данных $t = (1394, 1256, 1987, 439, 650, 724, 339, 2303, 810)$. Определить значение a для которого вектор $a^{-1}t (\mathrm{mod}\ p)$ — супервозрастающая последовательность. Найти исходных текст, который выглядит как бинарная последовательность.

Задача 65. Имеется конечное поле F порядка p^r. Пусть g — порождающий элемент его мультипликативной группы. Вычислить дискретный логарифм элемента f, если известно, что $\log_g(f^5) = k$, $\log_g(f^{11}) = t$.

Задача 66. Пусть дано конечное поле F_q. Предположим, что g — порождающий элемент его мультипликативной группы. Верны ли следующие свойства дискретного логарифма в группе F_q^*?

1. $\log_g(f_1 f_2) = \log_g(f_1) \log_g(f_2)$, 2. если $\log_g(f^2) = 2x$, то $\log_g(f) = x$.

Задача 67. Пусть $\mathbb{Z}_p$ — конечное простое поле, g — порождающий элемент его мультипликативной группы. Что можно сказать о дискретном логарифме x элемента f, если известно, что $f^{13} = 1$? Тот же вопрос для случая $f^{27} = 1$.

10. Криптосистема с открытым ключом Ривеста – Шамира – Адлемана

Задача 68. Пусть $n = pq$ – модуль системы RSA. Пусть e – открытый ключ шифрования. Предположим, что Боб знает порядок элемента e в группе $\mathbf{Z}^*_{\varphi(n)}$ и этот порядок равен k. Как Боб может дешифровать сообщение $m^e(mod n)$ и даже вычислить изначально секретный ключ d?

Задача 69. (Возможность использования общего модуля и распределения ключей RSA доверительным Центром.) Иногда RSA распределяется Центром, который, зафиксировав модуль $n = pq$, раздает пользователям ключи (e_i, d_i), $i = 1, ..., k$. Параметры p, q держатся Центром в секрете. Показать, что любой пользователь системы может определить все ключи d_i других пользователей за полиномиальное время.

Задача 70. (Неподвижные точки при шифровании RSA.) При шифровании в системе RSA $(n = pq, e, d)$ возможны совпадения шифровки c и исходного текста m. Покажите, что число совпадений равно $(1+$ нод$(p-1, e-1))(1+$нод $(q-1, e-1))$.

Какой вывод можно сделать для правильного выбора параметров p, q, e?

Задача 71. Пусть $n = pq$ – модуль системы RSA, e – открытый ключ шифрования. Предположим, что существует эффективный способ вычисления по шифровке любого текста $m \in \mathbf{Z}_n$ второго младшего бита ε_0 его двоичной записи. Можно ли аналогично тому, что было показано в пункте 5 данной лекции, определить по шифровке произвольный фиксированный текст m? Можно ли сделать то же самое, если мы умеем эффективно определять бит $\varepsilon_i, i \in \mathbf{N}$, любого текста m?

Задача 72. Пусть в системе RSA выполнено равенство $c^f = m(\mathrm{mod} n)$, где $c = m^e(\mathrm{mod} n)$ – шифровка. Можно ли утверждать, что $f = d$, где d – ключ дешифрования?

Задача 73. Алиса вычисляет (за деньги) аргумент m RSA-функции шифрования. То есть она получает при открытых данных (n, e) значение $c = m^e(\mathrm{mod} n)$ и после платежа сообщает обратившемуся величину m. Боб хочет расшифровать $c = m^e(\mathrm{mod} n)$, но он не желает, чтобы в процессе расшифровки Алиса узнала m. Описать, как Боб может организовать обращение к Алисе, чтобы в результате получить m, не раскрывая его значения для Алисы.

Задача 74. Допустим, что в системе RSA передана не только шифровка $c = m^e (\mathrm{mod} n)$, но и сообщение вида $\tilde{c} = m^{2^k} (\mathrm{mod} n)$. Может ли третье лицо прочитать сообщение m?

Задача 75. Модуль RSA равен $n = 24637$, открытый ключ $e = 3$. Вычислить ключ дешифрования d.

Задача 76. Модуль RSA равен $n = 1145941$, открытый ключ $e = 11$. Вычислить ключ дешифрования d.

Задача 77. В системе RSA с параметрами $(n = pq, e, d)$ $e^{11} = 1 (\mathrm{mod}(\phi(n))$. Чему равен d?

Задача 78. Доказать, что в системах RSA с модулями $n_1 = 21$ и $n_2 = 35$ все возможные ключи шифрования e совпадают с ключами дешифрования d.

Задача 79. При шифровании в системе RSA $(n = pq, e, d)$ оказалось, что повторное шифрование всегда приводит к исходному тексту. Как это объяснить? В чем причина? Привести пример конечного простого поля, в котором это свойство выполнено для любого ключа e.

Задача 80. Алиса сообщила Бобу открытые параметры $(n, e) = (56310949, 72)$, установленной у нее системы шифрования RSA. Боб выразил сомнение

по этому поводу. В чем заключается причина этого сомнения?

Задача 81. Предлагается следующее "обобщение" RSA. Пользователь устанавливает модуль RSA $n = pq$. Затем он выбирает два открытых ключа e_1, e_2, таких, что НОД$(e_1, e_2, \phi(n)) = 1$. При этом ключи e_1, e_2 не обязаны быть обратимыми $(\mathrm{mod}(\phi(n)))$. Получив сообщение m в виде пары вычетов $c_1 = m^{e_1}(\mathrm{mod}n)$, $c_2 = m^{e_2}(\mathrm{mod}n)$, он вычисляет $c_1^{d_1} c_2^{d_2} = m^{e_1 d_1 + e_2 d_2} = m(\mathrm{mod}n)$. Показать, что данная система равносильна RSA.

Задача 82. Дана система RSA, в которой $n = 12758351$, $e = 65537$. Зашифрован слово из 5 букв английского языка (обычный алфавит — 26 знаков). $m^e = 2309106(\mathrm{mod}n)$. Найти значение m и по его стандартной оцифровке в 26-ричной системе исходое слово.

Задача 83. Пусть дана система RSA с модулем $n = 77$. Сколько всего имеется ключей шифрования e? Сколько из них совпадает со своими ключами дешифрования d?

11. Простые числа

Задача 84. Математики в Древнем Китае считали, что число n является простым тогда и только тогда, когда n делит $2^n - 2$.

Доказать, что данное условие действительно является необходимым для простоты числа n. Более того, простое число n обязано делить разность $k^n - k$ при любом k.

Привести пример, показывающий его недостаточность. Другими словами, представить составное число n, тем не менее делящее $2^n - 2$.

Задача 85. Пусть p – простое число. Доказать, что

$$(p-1)! = -1(\mathrm{mod} p).$$

Этот результат известен как теорема Вильсона.

Задача 86. Пусть n – составное число, отличное от 4. Доказать, что

$$(n-1)! = 0(\mathrm{mod} n).$$

Задача 87. Пусть $a^n - 1$ – простое число. Доказать, что в этом случае $a = 2$ и n – тоже простое число.

Простые числа вида $a^p - 1, p$ простое, называются *числами Мерсенна.*

Задача 88. Пусть $a^n + 1$ – простое число. Доказать, что a четно и n является степенью 2.

Простые числа вида $2^{2^t} + 1$ называются *числами Ферма.*

12. Разложимость целых чисел на множители

Задача 89. Разложить на множители числа

$$n_1 = 21894583143407671,$$

$$n_2 = 317481472366756346287.$$

Задача 90. Найти простое число $p \geq 2^{100}$, такое, что $q = (p-1)/2$ – тоже простое.

Такие числа называются числами Софи Жермен.

Задача 91. Разложить на множители числа

$$n_1 = 57398617605606738780974553655371817744968877084487616807685915353903 24,$$

$$n_2 = 30004823012610422335343801599588688229540363958714487162565428757720061053669162994262636443794703397,$$

$$n_3 = 16604589036844609947075611165473677273146067100305915193876385419636008124704444102982413426026365453 7.$$

13. Алгоритмы генерации псевдослучайных последовательностей

Задача 92. Объяснить, почему при установке BBS-генератора требуется, чтобы простые числа p, q были сравнимы с $3(mod 4)$.

Задача 93. Вывести формулу для общего члена последовательности, порождаемой ЛКГ

$$x_{t+1} = ax_t + b(\mathrm{mod} n).$$

Задача 94. Выяснить, когда ЛКГ из предыдущей задачи порождает последовательность максимального периода.

Задача 95. Пусть задан МКГ

$$x_{t+1} = ax_t(\mathrm{mod} n).$$

Предположим, что нод$(x_0, n) = 1$. Каково возможное максимальное значение периода выпускной последовательности?

Задача 96. В кольце $\mathbb{Z}_{24}$ берем произвольный отличный от 0 вычет $s = s_0$ (посев). Строим

последовательность $s_0, s_1, \ldots$ по правилу $s_{i+1} = 7s_i \pmod{24}$ для $i \geq 0$. Чему равен период этой последовательности?

14. Поточные криптосистемы

Задача 97. Показать, что многочлен $f(D) = D^4+D^3+D^2+D+1 \in \mathbf{Z}_2[D]$ неприводим, но не примитивен. Чему равен период выпускной последовательности LFSR с таким связующим многочленом $f(D)$?

Задача 98. Проверить, будет ли многочлен $f(D) = D^4 + D + 1 \in \mathbf{Z}_2[D]$ неприводимым и примитивным.

Задача 99. Показать, что многочлен $f(D) = D^4+D^3+1 \in \mathbf{Z}_2[D]$ неприводим. Будет ли он примитивным? Чему равен период выпускной последовательности LFSR с таким связующим многочленом?

Задача 100. Проверить, что неприводимый многочлен $f(D) = D^5 + D^2 + 1 \in \mathbf{Z}_2[D]$ является примитивным. Убедиться, что в качестве связующего многочлена он дает выпускную последовательность максимального периода 31, выбрав вектором начальных содержаний $[1, 1, 1, 1, 1]$.

Задача 101. Построить LFSR максимального периода с 6-ю состояниями.

Задача 102. Следующая шифровка получена шифром Вернама, в котором ключ генерируется LFSR с длиной регистра 7:

$$0,1,1,0,0,0,1,0,1,0,1,1,1,0,0,1,1,1,0,1,0,1,0,0,0,1,0,0,0,1,1,$$

$$0,0,0,1,0,1,0,1,1,1,0,0,1,1,1,0,1,0,1.$$

Предположим, что известно начало исходного текста

$$1,0,0,1,0,0,1,0,0,1,0,0,1,0,0.$$

Найти весь исходный текст. Что можно было бы сказать при длине регистра 8?

Задача 103. Доказать, не используя вычислений, что любой неприводимый многочлен степени 5 над полем $\mathbb{Z}_2$ является примитивным.

Неприводимый многочлен $f(x) \in \mathbb{Z}_p[x]$ называется примитивным, если в построенном по нему поле порядка p^n, где n — степень многочлена, многочлен x (как элемент поля) порождает мультипликативную группу поля.

Задача 104. Доказать, что многочлен $f(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ не только неприводим, но и примитивен. Что можно сказать о многочлене $g(x) = x^5 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$?

Задача 105. Доказать, что многочлены $f(x) = x^4 + x^3 + x^2 + x + 1$ и $g(x) = x^4 + x + 1$ неприводимы над полем $\mathbb{Z}_2$. Один из них является примитивным. Какой многочлен примитивен?

Задача 106. Пусть выпускная последовательность бинарных символов начинается с задания содержаний $s_0 = 1, s_1 = 1, s_2 = 0, s_3 = 1$. Каждый последующий бит вычисляется по формуле: $s_{i+1} = s_i s_{i-1} + s_{i-3} s_{i-2}$, $i = 3, 4, \ldots$

Найти LFSR, задающий по тому же начальному заданию (при длине регистра 4) ту же самую последовательность.

Задача 107. Пусть выпускная последовательность бинарных символов начинается с задания содержаний $s_0 = 0, s_1 = 1, s_2 = 0, s_3 = 1$. Каждый последующий бит вычисляется по формуле: $s_{i+1} = s_i + s_{i-3} s_{i-2} + 1$, $i = 3, 4, \ldots$

Найти LFSR, задающий по тому же начальному заданию (при длине регистра 4) ту же самую последовательность.

Задача 108. Длина регистра 4. Начало выпускной последовательности 1011011. Найти связующий многочлен, если известно, что он несингулярен. Будет ли решение единственным?

Задача 109. Следующая шифровка получена шифров Вернама, в котором ключ генерируется LFSR длины регистра 7:

01100010101110011101010001000110001010111001110101.

Предположим, что известно начало исходного текста:

100100100100100. Найти весь исходный текст. Что можно было бы сказать при длине регистра 8?

15. Идентификация и аутентификация

Задача 110. В сети каждый пользователь A имеет свой открытый алгоритм шифрования E_A и секретный алгоритм дешифрования D_A. Сообщение m от A к B посылается в формате $(E_B(m), A)$. Адрес A говорит B, от кого пришло сообщение. Получатель B извлекает из сообщения m и автоматически посылает обратно по указанному адресу A сообщение $(E_A(m), B)$ в том же формате.

Покажите, что третий пользователь C, который может перехватывать сообщения и посылать их в правильном формате, способен извлечь сообщение m.

Задача 111. Показать, что изменение формата на $E_B(E_B(m), A), A)$ и автоматического ответа $E_A(E_A(m), B), B)$ не делает коммуникацию безопасной.

16. Электронные подписи

Задача 112. Рассмотрим следующее упрощение схемы Эль Гамаля. Пусть p – простое число, g – порождающий элемент мультипликативной группы $\mathbf{Z}_p^*$. Эти данные открыты.

Пользователь выбирает секретное число $1 \leq a \leq p-1$ и открывает значение $y = g^a (\mathrm{mod} p)$.

К сообщению $m \in \{0,1\}^*$ применяется известная хэш-функция, дающая значение $h = h(m) \in \mathbf{Z}_p$. Все, как в алгоритме Эль Гамаля.

Допустим, что нод$(h, p-1) = 1$. Этого можно добиться, внеся необходимые коррективы в случае невыполнения. Мы не уточняем, как это можно сделать.

При генерации подписи пользователь вычисляет значение

$$z = h^{-1} a (\mathrm{mod}(p-1)).$$

В качестве подписи под документом m предлагается использовать g^z.

Прверка правильности подписи элементарна:

$$(g^z)^h = g^{h^{-1}ha} = g^a (\mathrm{mod} p).$$

Подпись принимается, если полученное значение совпадет с y.

Объяснить, почему упомянутая схема неприемлема.

17. Электронные платежи

Задача 113. Привести схему заказа электронной карточки, в которой фиксируется имя владельца. Предполагается защищенность такой фиксации.

Задача 114. Привести схему электронных платежей, при которой банк-эмитент не владеет полной информацией об остатке средств на карточке. Он может лишь судить о достаточности остатка при очередном платеже.

18. Управление ключами

Задача 115. Предположим, что в некоторой структуре используется система шифрования, в которой, как, например, в DES (см. приложение 1), ключи K представляют собой бинарные последовательности фиксированной длины l (в DES эта длина равна 56). Предположим, что ключи хранятся в зашифрованном с использованием системы RSA виде, как

$$C = K^e (\mathrm{mod} n).$$

Здесь, как обычно, $n = pq$ – модуль системы RSA, e – открытый ключ шифра. Ключ K при этом рассматривается как число в двоичной записи. Показать, что с большой вероятностью ключ K может быть раскрыт путем перебора примерного объема $2^{l/2}$. Откуда появилась дополнительная слабость? Какое свойство натуральных чисел может быть использовано?

19. Эллиптические кривые

Задача 116. Проверить, что уравнение

$$y^2 = x^3 + 2x + 1$$

задает эллиптическую кривую E над полем $\mathbf{Z}_5$.

Найти все элементы группы $G(E)$. Привести таблицу сложения этих элементов. Какова алгебраическая структура этой группы? Будет ли она циклической?

Задача 117. Построить эллиптические кривые над полями $\mathbf{F}_{2^4}, \mathbf{F}_{13}, \mathbf{F}_{5^2}$, привести таблицы сложения для соответствующих групп. Какова их алгебраическая структура?

Задача 118. Привести примеры протоколов Диффи – Хеллмана и Масси – Омуры для эллиптических кривых над полямии $\mathbf{F}_5, \mathbf{F}_{13}, \mathbf{F}_{2^4}$.

Задача 119. Пусть E – эллиптическая кривая над полем $\mathbf{F}_{2^4}$, заданная уравнением $y^2 + y = x^3$. Показать, что для любой точки $P \in E$ имеет место равенство $3P = 0$. Это означает, что группа $G(E)$ имеет период 3.

Сколько точек содержит группа $G(E)$? Какова ее алгебраическая структура?

20. Алгебраическое шифрование

Задача 120. Привести конкретный пример разделения ключа в схеме Аншелm – Аншеля – Голдфилда.

Задача 121. Объяснить, почему использование вместо группы кос $\mathbf{B}_n$ свободной группы F_n в системе Аншель – Аншеля – Голдфилда не обладает достаточной криптостойкостью.

21. Стандарт шифрования DES

Задача 122. Пусть $D \subseteq \mathbf{S}_M$ – подмножество элементов группы $\mathbf{S}_M$ всех подстановок некоторого конечного множества M. Для любой пары элементов $d \in D$ и $m \in M$ определим наименьшее число $k = k(d, m)$, для которого $d^k(m) = m$. Доказать, что k делит порядок $|d|$ элемента $d \in \mathbf{S}_M$.

Задача 123. Проверить по одной из S-таблиц следующие свойства:

1) при фиксированных крайних битах 6-битового входа центральные 4-битовые блоки находятся во взаимно-однозначном соответствии с 4-битовыми выходами;

2) если входы отличаются только одним битом, то выходы отличаются не менее чем двумя битами.

22. Стандарты электронной подписи

Задача 124. Пусть $G = C_n$ – циклическая группа конечного порядка n, q – делитель n. Доказать, что в группе G существует единственная подгруппа $H = C_q$ порядка q.

Данное свойство используется при построении платформ описанных выше стандартов электронной подписи.

Задача 125. Предположим, что Алиса использует в системе DSA один и тот же «случайный» сессионный ключ k для подписи двух различных документов m_1 и m_2. Пусть эти подписи (r_1, s_1) и (r_2, s_2) соответственно. Предположим, что потенциальный взломщик Оскар знает как документы m_1, m_2, так и данные подписи. Показать, как Оскар может восстановить секретный ключ a.

Задача 126. Анна пользуется "детской" версией DSS с простым параметром $p = 43$, порождающим элементом $f = 21$ порядка 7. Случайно она подписывает сразу два документа, используя один и тот же сессионный ключ k. Хэшированные значения $h(m_1), h(m_2)$ для этих документов равны 2 и 3, соответственно. Подписи $(2, 1)$ и $(2, 6)$, соответственно. Определить долгосрочный ключ a.

23. Стандарт шифрования AES

Задача 127. Доказать неприводимость многочлена $f(x) = = x^8 + x^4 + x^3 + x + 1 \in \mathbf{Z}_2[x]$, по которому строится поле $\mathbf{F}_{2^8}$ в системе AES.

Задача 128. Пусть $g(y) \in \mathbf{Z}_2[y]$ – многочлен, определенный формулой (3.6). Указать явный вид многочлена $g'(y) \in \mathbf{Z}_2[y]$ такого, что

$$g(y)g'(y) = 1(\mathrm{mod}(y^4 + 1)).$$

Другими словами, дать явный вид многочлена $g(y)^{-1} \bmod (y^4 + 1)$.

Литература

1. *Агибалов Г.П.* Избранные теоремы начального курса криптографии: учебное пособие. – Томск: Изд-во науч.-техн. лит-ры, 2005. – 113 с.

2. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии: учебное пособие. – М.: Гелиос АРВ, 2002. – 480 с.

3. Введение в криптографию / под общ. ред. В.В. Ященко. – М.: МЦНМО: ЧеРо, 1999. – 272 с.

4. *Иванов М.А.* Криптография. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: Кудиц-образ, 2001. – 363 с.

5. *Кан Д.* Война кодов и шифров. История четырех тысячелетий криптографии. – М.: Рипол классик, 2004. – 526 с.

6. *Кнут Д.* Искусство программирования для ЭВМ. – М.: Мир, Т. 1. – 1976; Т. 2. – 1977; Т. 3. – 1978.

7. *Мао В.* Современная криптография: теория и практика. – М.: Вильямс, 2005. – 768 с.

8. *Марков А.А.* Основы алгебраической теории кос // Труды матем. ин-та АН СССР. 16 (1945).

9. *Романьков В.А.* Введение в криптографию: метод. указ. – Усть-Каменогорск: Изд-во ВКГУ, 2003. – 43 с.

10. *Н. Смарт.* Криптография. - М.: Техносфера, 2005. – 525 с.

12. *В. Столлингс.* Криптография и защита сетей. Принципы и практика. М.; СПб.; Киев: Вильямс, 2001. — 669 с.

13. *Фомичев В.М.* Дискретная математика и криптология. – М.: Диалог-МИФИ, 2003. - 397 с.

14. *Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В.* Математические и компьютерные основы криптологии: учебное пособие. – Минск: Новое знание, 2003. – 382 с.

15. *Шеннон К.* Работы по теории информации и кибернетике. – М.: ИЛ, 1963. – 830 с.

16. *Agrawal M., Kayal N., Saxena N.* Primes is in P. Annals of Math., 169 N2 (2004), 781–793.

17. *Alford W.R., Granville A., Pomerance C.* There are infinitely many Carmichael numbers. Annals of Math., 140 N 3 (1994), 703–722.

16. *Anshel I., Anshel M., Goldfeld G.* An algebraic method for public-key cryptography. Math. Res. Lett., 6 N3–4 (1999), 287–291.

18. *Birman J.S.* Braids, links, and mapping class groups. Annals Math. Stud., 82 (1974).

19. *Campbell K.W., Wiener M.J.* DES is not a group. Lect. Notes in Computer Science. Advances in Cryptology – Crypto'92, New York: Springer-Verlag, 512–520.

20. *Coppersmith D.* The real reason for Rivest's phenomenon. Lect. Notes in Computer Science. Advances in Cryptology. – Crypto '85, New York: Springer-Verlag, 535–536.

21. *Diffie W., Hellman M.E.* New directions in cryptography. IEEE Transaction Information Theory, 22 N 6 (1976), 644–654.

22. *ElCamal.* A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transaction on Informatoin Theory, 1985.

23. *Koblitz N.* A course in number theory and cryptography. Graduate texts in math. 114. – New-York: Springer-Verlag, 1994.

24. *Menezes A., Okamoto T., Vanstone S.A.* Reducing elliptic curve logarithms to logarithms in a finite field. In: Proc. of the 23rd Annual ACM Symp. on Theory of Computing, 1991, New Orlean, USA, ACM 1991, STOC 1991, 80–89.

25. *Menezes A., Oorschot P.C., Vanstone S.A.* Handbook of Applied Cryptography, CRC Press, 1966.

26. *Myasnikov A., Shpilrain V., Ushakov A.* Group-based cryptography. Advanced courses in mathematics CRM Barselona. – Basel-Boston-Berlin: Birkhäuser, 2008. 183 p.

27. *Rivest R.L., Shamir A., Adleman L.* A method for obtaining digital signatures and public-key cryptosystems.

Communications of the ACM, 21 N 2 (1978), 120–126.

28. *Waterhouse W.* Abelian varieties over finite fields. Ann. Sci. École Norm. Sup., 4^e série, 2 (1969), 521-560.