

The S/KEY One-Time Password System

Система одноразовых паролей S/KEY

Статус документа

Этот документ содержит информацию для сообщества Internet. Документ не задаёт каких-либо стандартов Internet. Допускается свободное распространение документа.

Аннотация

Этот документ описывает систему одноразовых паролей S/KEY*, выпущенную для общего пользования компанией Bellcore и описанную в [3]. Образец реализации и документация доступны для анонимного доступа (anonymous) по протоколу ftp на сайте ftp.bellcore.com в каталоге pub/nmh/...

Обзор

Одной из форм атак на компьютерную систему, подключённую к Internet, является прослушивание (перехват) сетевых соединений для получения идентификатора и пароля легитимного пользователя, имеющего доступ в систему. Перехваченное имя (login id) и пароль позволяют получить доступ в систему. Система одноразовых паролей S/KEY предназначена для противодействия атакам этого типа, называемым атаками с воспроизведением (replay attack).

Благодаря системе S/KEY пароль передаётся через сеть лишь один раз. Пользовательская секретная фраза никогда не передаётся в сеть даже при входе в систему или выполнении других команд, требующих проверки подлинности (аутентификации), таких как команды UNIX passwd и su. Таким образом, не возникает уязвимости к атакам с перехватом и воспроизведением. Повышение уровня безопасности обеспечивается тем, что секретную информацию не требуется хранить где-либо в системе, включая защищаемый хост.

Система S/KEY защищает от внешних пассивных атак на подсистему аутентификации. Она не препятствует перехвату злоумышленником частных сведений и не обеспечивает защиты от «внутренних заданий» и активных атак, где потенциальный злоумышленник может перехватывать и изменять поток пакетов.

Введение

Система одноразовых паролей S/KEY работает на двух сторонах. У клиента должен генерироваться подходящий одноразовый пароль, а на стороне хоста сервер должен проверять одноразовый пароль и разрешать смену секретной фразы пользователя.

Клиент системы S/KEY передаёт секретную фразу пользователя безопасной хэш-функции для создания одноразового пароля. При каждом использовании количество доступных применений сокращается на 1. Таким образом генерируется уникальная последовательность паролей. Хост системы S/KEY проверяет одноразовый пароль с помощью однократного вызова защищённой функции и сравнения результата с предыдущим одноразовым паролем. Этот метод был предложен Лесли Лэмпортом (Leslie Lamport) в работе [1].

Безопасная хэш-функция

Безопасной хэш-функцией является функция, которую легко выполнить в одном направлении, но вычислительно невозможно обратить. Система S/KEY основана на алгоритме цифрового дайджеста MD4 (Message Digest), разработанном Рональдом Ривестом (Ronald Rivest) [2]. С тех пор, как начато использование системы аутентификации S/KEY, был предложен алгоритм MD5. Применение алгоритма MD4 было сохранено в системе из-за большого числа клиентских программ, получивших распространение. Некоторые сайты создали похожие системы на основе MD5. Очевидно, что для совместимости клиенты и серверы должны использовать одну безопасную хэш-функцию.

Система S/KEY использует одноразовые пароли размером 64 бита. Этот размер считается достаточно большим для обеспечения безопасности и достаточно малым для ввода вручную при необходимости (см. ниже, Формы паролей).

Система S/KEY применяет безопасную хэш-функцию несколько раз для получения на выходе 64 битов. Функция MD4 принимает на входе произвольное число битов, давая на выходе 128 битов. Безопасная хэш-функция S/KEY заключается в применении MD4 к 64 битам входных данных и сворачивании выхода MD4 с помощью операции «исключительное ИЛИ» (exclusive or) в 64 бита.

Генерация одноразового пароля

В этом параграфе описан расчёт одноразового пароля S/KEY. На этапе подготовки выполняется объединение входных данных, на этапе генерации несколько раз применяется безопасная хэш-функция, а функция вывода отображает одноразовый 64-битовый пароль в читаемой форме.

Секретная парольная фраза клиента может иметь любой размер и следует использовать фразы не короче 8 символов. Поскольку описанная выше безопасная хэш-функция S/KEY принимает на входе 64 бита, требуется этап подготовки. На этом этапе выполняется конкатенация парольной фразы с затравкой (seed), которая передаётся с сервера в открытом виде (clear text). Эта несекретная затравка позволяет клиенту использовать одну секретную фразу на нескольких машинах (использующих разные затравки). Для удобства синтаксического анализа в значении seed не допускается наличие символов пробела и следует применять только буквы и цифры. Результат конкатенации передаётся на вход

MD4, а выход функции сокращается до 64 битов с помощью операции exclusive-OR (XOR) для двух 8-байтовых половин.

Ниже приведён фрагмент кода, определяющего этап подготовки с использованием реализации MD4 из RFC 1320 [2].

```
strcpy(buf,seed);
strcat(buf,passwd);
MDbegin(&md)
MDupdate(&md,(unsigned char *)buf,8*buflen);

/* Сокращение до 64 битов */
md.buffer[0] ^= md.buffer[2];
md.buffer[1] ^= md.buffer[3];
```

Последовательность одноразовых паролей создаётся путём многократного применения безопасной хэш-функции к результату предварительного этапа (S). Первый одноразовый пароль создаётся путём применения безопасной хэш-функции к S заданное пользователем число раз (N). При создании следующего одноразового пароля безопасная хэш-функция применяется к S на 1 раз меньше (N-1) и т. д. Злоумышленник, который перехватил передачу одноразового пароля не сможет создать следующий пароль, поскольку для этого потребуется обратить хэш-функцию.

Формы паролей

Описанная выше процедура генерирует одноразовые пароли размером 64 бита. Вводить 64-битовые числа сложно и при этом могут возникать ошибки. Некоторые программы-калькуляторы системы одноразовых паролей S/KEY помещают полученный пароль во входной поток данных, а другие делают доступным для системных функций «вырезания и вставки» (cut and paste). В некоторых случаях требуется вводить пароль вручную. Система S/KEY разработана для упрощения ручного ввода без создания препятствий методам автоматического ввода. Одноразовый пароль преобразуется в последовательность из 6 коротких (1 - 4 буквы) английских слов, выбираемых из словаря в 2048 слов. При 11 битах на слово можно закодировать таким способом все одноразовые пароли. Для обеспечения совместимости требуется использовать для всех хостов и калькуляторов системы S/KEY общий словарь. Такой словарь приведён в конце этого RFC.

Проверка одноразового пароля

Предполагается, что функция хост-системы, требующая аутентификации S/KEY, будет выдавать запрос S/KEY (challenge). Этот запрос предоставит клиенту текущие параметры S/KEY - порядковый номер и заправку (seed). Для запроса S/KEY важно использование стандартного формата, чтобы автоматизированные клиенты (см. ниже) могли распознать запрос и извлечь из него параметры. Формат запроса показан ниже.

```
s/key sequence_integer seed
```

Три компонента (token) запроса разделены одиночными пробелами, завершается запрос пробелом или символом новой строки.

Имея параметры и секретную фразу, клиент может рассчитать (или посмотреть) одноразовый пароль, который он затем передаёт хосту, где пароль можно проверить.

В хост-системе имеется файл (в эталонной реализации UNIX это /etc/skeykeys), содержащий для каждого пользователя значение одноразового пароля при последнем успешном входе в систему, или этот файл может быть инициализирован для первого входа с одноразовым паролем из последовательности с помощью команды keyinit (имя команды может зависеть от реализации). Для аутентификации полученный одноразовый пароль передаётся (1 раз) функции безопасного хеширования. Если результат совпадает с сохранённым предыдущим одноразовым паролем, аутентификация считается успешной и полученный одноразовый пароль записывается в файл для последующего использования.

Поскольку число применений хэш-функции клиентом каждый раз уменьшается на 1, в какой-то момент пользователь должен будет заново инициализировать систему, иначе следующий вход будет неудачным. Инициализация выполняется с помощью команды keyinit, которая позволяет изменить секретную парольную фразу, счётчик итераций и заправку (seed). Распространённым методом является инкрементирование цифры (цифр) в конце seed и переустановка значения счётчика итераций (что-то из диапазоны 500-1000).

Клиенты

Доступно несколько программ для расчёта одноразовых паролей S/KEY. В эталонную реализацию включены командный интерфейс (CLI) для UNIX и PC (key), интерфейсы TSR¹ для PC (ctkey, termkey, porkey) и интерфейсы GUI для Macintosh и Windows (keyapp и безымянный интерфейс Macintosh).

Самый простой расчёт обеспечивает команда вида

```
key [-n count] sequence seed
```

Необязательный параметр count служит для отображения нескольких одноразовых паролей, что может быть полезным для создания бумажного списка одноразовых паролей.

Наиболее автоматизированным вариантом является резидентная (TSR) программа termkey для PC. Программа сканирует экран в поисках параметров S/KEY, приглашает ввести секретную парольную фразу и передаёт одноразовый пароль в буфер клавиатуры.

Благодарности

Идея проверки подлинности с помощью S/KEY была предложена Лесли Лэмпортом (Leslie Lamport) [1]. Описанную здесь систему предложил Фил Кэрн (Phil Karn), который также написал код большей части реализации.

¹Terminate and Stay Resident - завершиться и остаться резидентной в памяти.

Литература

- [1] Lamport, L., "Password Authentication with Insecure Communication", Communications of the ACM 24.11, November 1981, 770-772.
- [2] Rivest, R., "The MD4 Message-Digest Algorithm", [RFC 1320](#), MIT and RSA Data Security, Inc., April 1992
- [3] Haller, N., "The S/KEY One-Time Password System", Proceedings of the ISOC Symposium on Network and Distributed System Security, February 1994, San Diego, CA
- [4] Haller, N., and R. Atkinson, "On Internet Authentication", RFC 1704, Bell Communications Research and Naval Research Laboratory, October 1994

Вопросы безопасности

Документ целиком посвящён вопросам безопасности.

Адрес автора

Neil Haller
Bellcore
MRE 2Q-280
445 South Street
Morristown, NJ, 07960-6438, USA
Phone: +1 201 829-4478
Fax: +1 201 829-2504
EMail: nmh@bellcore.com

Словарь для преобразования между S/KEY 6-Word и двоичным форматом

Это словарь из файла put.c. Код этого модуля и реализация S/KEY One Time Password System доступны анонимно на сайте <ftp.bellcore.com> в каталоге pub/nmh/skey.

```
{
  "A",      "ABE",  "ACE",  "ACT",  "AD",   "ADA",  "ADD",
  "AGO",    "AID",  "AIM",  "AIR",  "ALL",  "ALP",  "AM",   "AMY",
  "AN",     "ANA",  "AND",  "ANN",  "ANT",  "ANY",  "APE",  "APS",
  "APT",    "ARC",  "ARE",  "ARK",  "ARM",  "ART",  "AS",   "ASH",
  "ASK",    "AT",   "ATE",  "AUG",  "AUK",  "AVE",  "AWE",  "AWK",
  "AWL",    "AWN",  "AX",   "AYE",  "BAD",  "BAG",  "BAH",  "BAM",
  "BAN",    "BAR",  "BAT",  "BAY",  "BE",   "BED",  "BEE",  "BEG",
  "BEN",    "BET",  "BEY",  "BIB",  "BID",  "BIG",  "BIN",  "BIT",
  "BOB",    "BOG",  "BON",  "BOO",  "BOP",  "BOW",  "BOY",  "BUB",
  "BUD",    "BUG",  "BUM",  "BUN",  "BUS",  "BUT",  "BUY",  "BY",
  "BYE",    "CAB",  "CAL",  "CAM",  "CAN",  "CAP",  "CAR",  "CAT",
  "CAW",    "COD",  "COG",  "COL",  "CON",  "COO",  "COP",  "COT",
  "COW",    "COY",  "CRY",  "CUB",  "CUE",  "CUP",  "CUR",  "CUT",
  "DAB",    "DAD",  "DAM",  "DAN",  "DAY",  "DEE",  "DEL",
  "DEN",    "DES",  "DEW",  "DID",  "DIE",  "DIG",  "DIN",  "DIP",
  "DO",     "DOE",  "DOG",  "DON",  "DOT",  "DOW",  "DRY",  "DUB",
  "DUD",    "DUE",  "DUG",  "DUN",  "EAR",  "EAT",  "ED",   "EEL",
  "EGG",    "EGO",  "ELI",  "ELK",  "ELM",  "ELY",  "EM",   "END",
  "EST",    "ETC",  "EVA",  "EVE",  "EWE",  "EYE",  "FAD",  "FAN",
  "FAR",    "FAT",  "FAY",  "FED",  "FEE",  "FEW",  "FIB",  "FIG",
  "FIN",    "FIR",  "FIT",  "FLO",  "FLY",  "FOE",  "FOG",  "FOR",
  "FRY",    "FUM",  "FUN",  "FUR",  "GAB",  "GAD",  "GAG",  "GAL",
  "GAM",    "GAP",  "GAS",  "GAY",  "GEE",  "GEL",  "GEM",  "GET",
  "GIG",    "GIL",  "GIN",  "GO",   "GOT",  "GUM",  "GUN",  "GUS",
  "GUT",    "GUY",  "GYM",  "GYP",  "HA",   "HAD",  "HAL",  "HAM",
  "HAN",    "HAP",  "HAS",  "HAT",  "HAW",  "HAY",  "HE",   "HEM",
  "HEN",    "HER",  "HEW",  "HEY",  "HI",   "HID",  "HIM",  "HIP",
  "HIS",    "HIT",  "HO",   "HOB",  "HOC",  "HOE",  "HOG",  "HOP",
  "HOT",    "HOW",  "HUB",  "HUE",  "HUG",  "HUH",  "HUM",  "HUT",
  "I",      "ICY",  "IDA",  "IF",   "IKE",  "ILL",  "INK",  "INN",
  "IO",     "ION",  "IQ",   "IRA",  "IRE",  "IRK",  "IS",   "IT",
  "ITS",    "IVY",  "JAB",  "JAG",  "JAM",  "JAN",  "JAR",  "JAW",
  "JAY",    "JET",  "JIG",  "JIM",  "JO",   "JOB",  "JOE",  "JOG",
  "JOT",    "JOY",  "JUG",  "JUT",  "KAY",  "KEG",  "KEN",  "KEY",
  "KID",    "KIM",  "KIN",  "KIT",  "LA",   "LAB",  "LAC",  "LAD",
  "LAG",    "LAM",  "LAP",  "LAW",  "LAY",  "LEA",  "LED",  "LEE",
  "LEG",    "LEN",  "LEO",  "LET",  "LEW",  "LID",  "LIE",  "LIN",
  "LIP",    "LIT",  "LO",   "LOB",  "LOG",  "LOP",  "LOS",  "LOT",
  "LOU",    "LOW",  "LOY",  "LUG",  "LYE",  "MA",   "MAC",  "MAD",
  "MAE",    "MAN",  "MAO",  "MAP",  "MAT",  "MAW",  "MAY",  "ME",
  "MEG",    "MEL",  "MEN",  "MET",  "MEW",  "MID",  "MIN",  "MIT",
  "MOB",    "MOD",  "MOE",  "MOO",  "MOP",  "MOS",  "MOT",  "MOW",
  "MUD",    "MUG",  "MUM",  "MY",   "NAB",  "NAG",  "NAN",  "NAP",
  "NAT",    "NAY",  "NE",   "NED",  "NEE",  "NET",  "NEW",  "NIB",
  "NIL",    "NIP",  "NIT",  "NO",   "NOB",  "NOD",  "NON",  "NOR",
  "NOT",    "NOV",  "NOW",  "NU",   "NUN",  "NUT",  "O",    "OAF",
  "OAK",    "OAR",  "OAT",  "ODD",  "ODE",  "OF",   "OFF",  "OFT",
  "OH",     "OIL",  "OK",   "OLD",  "ON",   "ONE",  "OR",   "ORB",
  "ORE",    "ORR",  "OS",   "OTT",  "OUR",  "OUT",  "OVA",  "OW",
  "OWE",    "OWL",  "OWN",  "OX",   "PA",   "PAD",  "PAL",  "PAM",
  "PAN",    "PAP",  "PAR",  "PAT",  "PAW",  "PAY",  "PEA",  "PEG",
  "PEN",    "PEP",  "PER",  "PET",  "PEW",  "PHI",  "PI",   "PIE",
  "PIN",    "PIT",  "PLY",  "PO",   "POD",  "POE",  "POP",  "POT",
}
```

"POW",	"PRO",	"PRY",	"PUB",	"PUG",	"PUN",	"PUP",	"PUT",
"QUO",	"RAG",	"RAM",	"RAN",	"RAP",	"RAT",	"RAW",	"RAY",
"REB",	"RED",	"REP",	"RET",	"RIB",	"RID",	"RIG",	"RIM",
"RIO",	"RIP",	"ROB",	"ROD",	"ROE",	"RON",	"ROT",	"ROW",
"ROY",	"RUB",	"RUE",	"RUG",	"RUM",	"RUN",	"RYE",	"SAC",
"SAD",	"SAG",	"SAL",	"SAM",	"SAN",	"SAP",	"SAT",	"SAW",
"SAY",	"SEA",	"SEC",	"SEE",	"SEN",	"SET",	"SEW",	"SHE",
"SHY",	"SIN",	"SIP",	"SIR",	"SIS",	"SIT",	"SKI",	"SKY",
"SLY",	"SO",	"SOB",	"SOD",	"SON",	"SOP",	"SOW",	"SOY",
"SPA",	"SPY",	"SUB",	"SUD",	"SUE",	"SUM",	"SUN",	"SUP",
"TAB",	"TAD",	"TAG",	"TAN",	"TAP",	"TAR",	"TEA",	"TED",
"TEE",	"TEN",	"THE",	"THY",	"TIC",	"TIE",	"TIM",	"TIN",
"TIP",	"TO",	"TOE",	"TOG",	"TOM",	"TON",	"TOO",	"TOP",
"TOW",	"TOY",	"TRY",	"TUB",	"TUG",	"TUM",	"TUN",	"TWO",
"UN",	"UP",	"US",	"USE",	"VAN",	"VAT",	"VET",	"VIE",
"WAD",	"WAG",	"WAR",	"WAS",	"WAY",	"WE",	"WEB",	"WED",
"WEE",	"WET",	"WHO",	"WHY",	"WIN",	"WIT",	"WOK",	"WON",
"WOO",	"WOW",	"WRY",	"WU",	"YAM",	"YAP",	"YAW",	"YE",
"YEA",	"YES",	"YET",	"YOU",	"ABED",	"ABEL",	"ABET",	"ABLE",
"ABUT",	"ACHE",	"ACID",	"ACME",	"ACRE",	"ACTA",	"ACTS",	"ADAM",
"ADDS",	"ADEN",	"AFAR",	"AFRO",	"AGEE",	"AHAM",	"AHOY",	"AIDA",
"AIDE",	"AIDS",	"AIRY",	"AJAR",	"AKIN",	"ALAN",	"ALEC",	"ALGA",
"ALIA",	"ALLY",	"ALMA",	"ALOE",	"ALSO",	"ALTO",	"ALUM",	"ALVA",
"AMEN",	"AMES",	"AMID",	"AMMO",	"AMOK",	"AMOS",	"AMRA",	"ANDY",
"ANEW",	"ANNA",	"ANNE",	"ANTE",	"ANTI",	"AQUA",	"ARAB",	"ARCH",
"AREA",	"ARGO",	"ARID",	"ARMY",	"ARTS",	"ARTY",	"ASIA",	"ASKS",
"ATOM",	"AUNT",	"AURA",	"AUTO",	"AVER",	"AVID",	"AVIS",	"AVON",
"AVOW",	"AWAY",	"AWRY",	"BABE",	"BABY",	"BACH",	"BACK",	"BADE",
"BAIL",	"BAIT",	"BAKE",	"BALD",	"BALE",	"BALI",	"BALK",	"BALL",
"BALM",	"BAND",	"BANE",	"BANG",	"BANK",	"BARB",	"BARD",	"BARE",
"BARK",	"BARN",	"BARR",	"BASE",	"BASH",	"BASK",	"BASS",	"BATE",
"BATH",	"BAWD",	"BAWL",	"BEAD",	"BEAK",	"BEAM",	"BEAN",	"BEAR",
"BEAT",	"BEAU",	"BECK",	"BEEF",	"BEEN",	"BEER",	"BEET",	"BELA",
"BELL",	"BELT",	"BEND",	"BENT",	"BERG",	"BERN",	"BERT",	"BESS",
"BEST",	"BETA",	"BETH",	"BHOY",	"BIAS",	"BIDE",	"BIEN",	"BILE",
"BILK",	"BILL",	"BIND",	"BING",	"BIRD",	"BITE",	"BITS",	"BLAB",
"BLAT",	"BLED",	"BLEW",	"BLOB",	"BLOC",	"BLOT",	"BLOW",	"BLUE",
"BLUM",	"BLUR",	"BOAR",	"BOAT",	"BOCA",	"BOCK",	"BODE",	"BODY",
"BOGY",	"BOHR",	"BOIL",	"BOLD",	"BOLO",	"BOLT",	"BOMB",	"BONA",
"BOND",	"BONE",	"BONG",	"BONN",	"BONY",	"BOOK",	"BOOM",	"BOON",
"BOOT",	"BORE",	"BORG",	"BORN",	"BOSE",	"BOSS",	"BOTH",	"BOUT",
"BOWL",	"BOYD",	"BRAD",	"BRAE",	"BRAG",	"BRAN",	"BRAY",	"BRED",
"BREW",	"BRIG",	"BRIM",	"BROW",	"BUCK",	"BUDD",	"BUFF",	"BULB",
"BULK",	"BULL",	"BUNK",	"BUNT",	"BUOY",	"BURG",	"BURL",	"BURN",
"BURR",	"BURT",	"BURY",	"BUSH",	"BUSS",	"BUST",	"BUSY",	"BYTE",
"CADY",	"CAFE",	"CAGE",	"CAIN",	"CAKE",	"CALF",	"CALL",	"CALM",
"CAME",	"CANE",	"CANT",	"CARD",	"CARE",	"CARL",	"CARR",	"CART",
"CASE",	"CASH",	"CASK",	"CAST",	"CAVE",	"CEIL",	"CELL",	"CENT",
"CERN",	"CHAD",	"CHAR",	"CHAT",	"CHAW",	"CHEF",	"CHEN",	"CHEW",
"CHIC",	"CHIN",	"CHOU",	"CHOW",	"CHUB",	"CHUG",	"CHUM",	"CITE",
"CITY",	"CLAD",	"CLAM",	"CLAN",	"CLAW",	"CLAY",	"CLOD",	"CLOG",
"CLOT",	"CLUB",	"CLUE",	"COAL",	"COAT",	"COCA",	"COCK",	"COCO",
"CODA",	"CODE",	"CODY",	"COED",	"COIL",	"COIN",	"COKE",	"COLA",
"COLD",	"COLT",	"COMA",	"COMB",	"COME",	"COOK",	"COOL",	"COON",
"COOT",	"CORD",	"CORE",	"CORK",	"CORN",	"COST",	"COVE",	"COWL",
"CRAB",	"CRAG",	"CRAM",	"CRAY",	"CREW",	"CRIB",	"CROW",	"CRUD",
"CUBA",	"CUBE",	"CUFF",	"CULL",	"CULT",	"CUNY",	"CURB",	"CURD",
"CURE",	"CURL",	"CURT",	"CUTS",	"DADE",	"DALE",	"DAME",	"DANA",
"DANE",	"DANG",	"DANK",	"DARE",	"DARK",	"DARN",	"DART",	"DASH",
"DATA",	"DATE",	"DAVE",	"DAVY",	"DAWN",	"DAYS",	"DEAD",	"DEAF",
"DEAL",	"DEAN",	"DEAR",	"DEBT",	"DECK",	"DEED",	"DEEM",	"DEER",
"DEFT",	"DEFY",	"DELL",	"DENT",	"DENY",	"DESK",	"DIAL",	"DICE",
"DIED",	"DIET",	"DIME",	"DINE",	"DING",	"DINT",	"DIRE",	"DIRT",
"DISC",	"DISH",	"DISK",	"DIVE",	"DOCK",	"DOES",	"DOLE",	"DOLL",
"DOLT",	"DOME",	"DONE",	"DOOM",	"DOOR",	"DORA",	"DOSE",	"DOTE",
"DOUG",	"DOUR",	"DOVE",	"DOWN",	"DRAB",	"DRAG",	"DRAM",	"DRAW",
"DREW",	"DRUB",	"DRUG",	"DRUM",	"DUAL",	"DUCK",	"DUCT",	"DUEL",
"DUET",	"DUKE",	"DULL",	"DUMB",	"DUNE",	"DUNK",	"DUSK",	"DUST",
"DUTY",	"EACH",	"EARL",	"EARN",	"EASE",	"EAST",	"EASY",	"EBEN",
"ECHO",	"EDDY",	"EDEN",	"EDGE",	"EDGY",	"EDIT",	"EDNA",	"EGAN",
"ELAN",	"ELBA",	"ELLA",	"ELSE",	"EMIL",	"EMIT",	"EMMA",	"ENDS",
"ERIC",	"EROS",	"EVEN",	"EVER",	"EVIL",	"EYED",	"FACE",	"FACT",
"FADE",	"FAIL",	"FAIN",	"FAIR",	"FAKE",	"FALL",	"FAME",	"FANG",
"FARM",	"FAST",	"FATE",	"FAWN",	"FEAR",	"FEAT",	"FEED",	"FEEL",
"FEET",	"FELL",	"FELT",	"FEND",	"FERN",	"FEST",	"FEUD",	"FIEF",
"FIGS",	"FILE",	"FILL",	"FILM",	"FIND",	"FINE",	"FINK",	"FIRE",
"FIRM",	"FISH",	"FISK",	"FIST",	"FITS",	"FIVE",	"FLAG",	"FLAK",
"FLAM",	"FLAT",	"FLAW",	"FLEA",	"FLED",	"FLEW",	"FLIT",	"FLOC",
"FLOG",	"FLOW",	"FLUB",	"FLUE",	"FOAL",	"FOAM",	"FOGY",	"FOIL",
"FOLD",	"FOLK",	"FOND",	"FONT",	"FOOD",	"FOOL",	"FOOT",	"FORD",
"FORE",	"FORK",	"FORM",	"FORT",	"FOSS",	"FOUL",	"FOUR",	"FOWL",
"FRAU",	"FRAY",	"FRED",	"FREE",	"FRET",	"FREY",	"FROG",	"FROM",
"FUEL",	"FULL",	"FUME",	"FUND",	"FUNK",	"FURY",	"FUSE",	"FUSS",
"GAFF",	"GAGE",	"GAIL",	"GAIN",	"GAIT",	"GALA",	"GALE",	"GALL",
"GALT",	"GAME",	"GANG",	"GARB",	"GARY",	"GASH",	"GATE",	"GAUL",
"GAUR",	"GAVE",	"GAWK",	"GEAR",	"GELD",	"GENE",	"GENT",	"GERM",

"GETS",	"GIBE",	"GIFT",	"GILD",	"GILL",	"GILT",	"GINA",	"GIRD",
"GIRL",	"GIST",	"GIVE",	"GLAD",	"GLEE",	"GLEN",	"GLIB",	"GLOB",
"GLOM",	"GLOW",	"GLUE",	"GLUM",	"GLUT",	"GOAD",	"GOAL",	"GOAT",
"GOER",	"GOES",	"GOLD",	"GOLF",	"GONE",	"GONG",	"GOOD",	"GOOF",
"GORE",	"GORY",	"GOSH",	"GOUT",	"GOWN",	"GRAB",	"GRAD",	"GRAY",
"GREG",	"GREW",	"GREY",	"GRID",	"GRIM",	"GRIN",	"GRIT",	"GROW",
"GRUB",	"GULF",	"GULL",	"GUNK",	"GURU",	"GUSH",	"GUST",	"GWEN",
"GWYN",	"HAAG",	"HAAS",	"HACK",	"HAIL",	"HAIR",	"HALE",	"HALF",
"HALL",	"HALO",	"HALT",	"HAND",	"HANG",	"HANK",	"HANS",	"HARD",
"HARK",	"HARM",	"HART",	"HASH",	"HAST",	"HATE",	"HATH",	"HAUL",
"HAVE",	"HAWK",	"HAYS",	"HEAD",	"HEAL",	"HEAR",	"HEAT",	"HEBE",
"HECK",	"HEED",	"HEEL",	"HEFT",	"HELD",	"HELL",	"HELM",	"HERB",
"HERD",	"HERE",	"HERO",	"HERS",	"HESS",	"HEWN",	"HICK",	"HIDE",
"HIGH",	"HIKE",	"HILL",	"HILT",	"HIND",	"HINT",	"HIRE",	"HISS",
"HIVE",	"HOB",	"HOCK",	"HOFF",	"HOLD",	"HOLE",	"HOLM",	"HOLT",
"HOME",	"HONE",	"HONK",	"HOOD",	"HOOF",	"HOOK",	"HOOT",	"HORN",
"HOSE",	"HOST",	"HOUR",	"HOVE",	"HOWE",	"HOWL",	"HOYT",	"HUCK",
"HUED",	"HUFF",	"HUGE",	"HUGH",	"HUGO",	"HULK",	"HULL",	"HUNK",
"HUNT",	"HURD",	"HURL",	"HURT",	"HUSH",	"HYDE",	"HYMN",	"IBIS",
"ICON",	"IDEA",	"IDLE",	"IFFY",	"INCA",	"INCH",	"INTO",	"IONS",
"IOTA",	"IOWA",	"IRIS",	"IRMA",	"IRON",	"ISLE",	"ITCH",	"ITEM",
"IVAN",	"JACK",	"JADE",	"JAIL",	"JAKE",	"JANE",	"JAVA",	"JEAN",
"JEFF",	"JERK",	"JESS",	"JEST",	"JIBE",	"JILL",	"JILT",	"JIVE",
"JOAN",	"JOBS",	"JOCK",	"JOEL",	"JOEY",	"JOHN",	"JOIN",	"JOKE",
"JOLT",	"JOVE",	"JUDD",	"JUDE",	"JUDO",	"JUDY",	"JUJU",	"JUKE",
"JULY",	"JUNE",	"JUNK",	"JUNO",	"JURY",	"JUST",	"JUTE",	"KAHN",
"KALE",	"KANE",	"KANT",	"KARL",	"KATE",	"KEEL",	"KEEN",	"KENO",
"KENT",	"KERN",	"KERR",	"KEYS",	"KICK",	"KILL",	"KIND",	"KING",
"KIRK",	"KISS",	"KITE",	"KLAN",	"KNEE",	"KNEW",	"KNIT",	"KNOB",
"KNOT",	"KNOW",	"KOCH",	"KONG",	"KUDO",	"KURD",	"KURT",	"KYLE",
"LACE",	"LACK",	"LACY",	"LADY",	"LAID",	"LAIN",	"LAIR",	"LAKE",
"LAMB",	"LAME",	"LAND",	"LANE",	"LANG",	"LARD",	"LARK",	"LASS",
"LAST",	"LATE",	"LAUD",	"LAVA",	"LAWN",	"LAWS",	"LAYS",	"LEAD",
"LEAF",	"LEAK",	"LEAN",	"LEAR",	"LEEK",	"LEER",	"LEFT",	"LEND",
"LENS",	"LENT",	"LEON",	"LESK",	"LESS",	"LEST",	"LETS",	"LIAR",
"LICE",	"LICK",	"LIED",	"LIEN",	"LIES",	"LIEU",	"LIFE",	"LIFT",
"LIKE",	"LILA",	"LILT",	"LILY",	"LIMA",	"LIMB",	"LIME",	"LIND",
"LINE",	"LINK",	"LINT",	"LION",	"LISA",	"LIST",	"LIVE",	"LOAD",
"LOAF",	"LOAM",	"LOAN",	"LOCK",	"LOFT",	"LOGE",	"LOIS",	"LOLA",
"LONE",	"LONG",	"LOOK",	"LOON",	"LOOT",	"LORD",	"LORE",	"LOSE",
"LOSS",	"LOST",	"LOUD",	"LOVE",	"LOWE",	"LUCK",	"LUCY",	"LUGE",
"LUKE",	"LULU",	"LUND",	"LUNG",	"LURA",	"LURE",	"LURK",	"LUSH",
"LUST",	"LYLE",	"LYNN",	"LYON",	"LYRA",	"MACE",	"MADE",	"MAGI",
"MAID",	"MAIL",	"MAIN",	"MAKE",	"MALE",	"MALI",	"MALL",	"MALT",
"MANA",	"MANN",	"MANY",	"MARC",	"MARE",	"MARK",	"MARS",	"MART",
"MARY",	"MASH",	"MASK",	"MASS",	"MAST",	"MATE",	"MATH",	"MAUL",
"MAYO",	"MEAD",	"MEAL",	"MEAN",	"MEAT",	"MEEK",	"MEET",	"MELD",
"MELT",	"MEMO",	"MEND",	"MENU",	"MERT",	"MESH",	"MESS",	"MICE",
"MIKE",	"MILD",	"MILE",	"MILK",	"MILL",	"MILT",	"MIMI",	"MIND",
"MINE",	"MINI",	"MINK",	"MINT",	"MIRE",	"MISS",	"MIST",	"MITE",
"MITT",	"MOAN",	"MOAT",	"MOCK",	"MODE",	"MOLD",	"MOLE",	"MOLL",
"MOLT",	"MONA",	"MONK",	"MONT",	"MOOD",	"MOON",	"MOOR",	"MOOT",
"MORE",	"MORN",	"MORT",	"MOSS",	"MOST",	"MOTH",	"MOVE",	"MUCH",
"MUCK",	"MUDD",	"MUFF",	"MULE",	"MULL",	"MURK",	"MUSH",	"MUST",
"MUTE",	"MUTT",	"MYRA",	"MYTH",	"NAGY",	"NAIL",	"NAIR",	"NAME",
"NARY",	"NASH",	"NAVE",	"NAVY",	"NEAL",	"NEAR",	"NEAT",	"NECK",
"NEED",	"NEIL",	"NELL",	"NEON",	"NERO",	"NESS",	"NEST",	"NEWS",
"NEWT",	"NIBS",	"NICE",	"NICK",	"NILE",	"NINA",	"NINE",	"NOAH",
"NODE",	"NOEL",	"NOLL",	"NONE",	"NOOK",	"NOON",	"NORM",	"NOSE",
"NOTE",	"NOUN",	"NOVA",	"NUDE",	"NULL",	"NUMB",	"OATH",	"OBEY",
"OBOE",	"ODIN",	"OHIO",	"OILY",	"OINT",	"OKAY",	"OLAF",	"OLDY",
"OLGA",	"OLIN",	"OMAN",	"OMEN",	"OMIT",	"ONCE",	"ONES",	"ONLY",
"ONTO",	"ONUS",	"ORAL",	"ORGY",	"OSLO",	"OTIS",	"OTTO",	"OUCH",
"OUST",	"OUTS",	"OVAL",	"OVEN",	"OVER",	"OWLY",	"OWNS",	"QUAD",
"QUIT",	"QUOD",	"RACE",	"RACK",	"RACY",	"RAFT",	"RAGE",	"RAID",
"RAIL",	"RAIN",	"RAKE",	"RANK",	"RANT",	"RARE",	"RASH",	"RATE",
"RAVE",	"RAYS",	"READ",	"REAL",	"REAM",	"REAR",	"RECK",	"REED",
"REEF",	"REEK",	"REEL",	"REID",	"REIN",	"RENA",	"REND",	"RENT",
"REST",	"RICE",	"RICH",	"RICK",	"RIDE",	"RIFT",	"RILL",	"RIME",
"RING",	"RINK",	"RISE",	"RISK",	"RITE",	"ROAD",	"ROAM",	"ROAR",
"ROBE",	"ROCK",	"RODE",	"ROIL",	"ROLL",	"ROME",	"ROOD",	"ROOF",
"ROOK",	"ROOM",	"ROOT",	"ROSA",	"ROSE",	"ROSS",	"ROSY",	"ROTH",
"ROUT",	"ROVE",	"ROWE",	"ROWS",	"RUBE",	"RUBY",	"RUDE",	"RUDY",
"RUIN",	"RULE",	"RUNG",	"RUNS",	"RUNT",	"RUSE",	"RUSH",	"RUSK",
"RUSS",	"RUST",	"RUTH",	"SACK",	"SAFE",	"SAGE",	"SAID",	"SAIL",
"SALE",	"SALK",	"SALT",	"SAME",	"SAND",	"SANE",	"SANG",	"SANK",
"SARA",	"SAUL",	"SAVE",	"SAYS",	"SCAN",	"SCAR",	"SCAT",	"SCOT",
"SEAL",	"SEAM",	"SEAR",	"SEAT",	"SEED",	"SEEK",	"SEEM",	"SEEN",
"SEES",	"SELF",	"SELL",	"SEND",	"SENT",	"SETS",	"SEWN",	"SHAG",
"SHAM",	"SHAW",	"SHAY",	"SHED",	"SHIM",	"SHIN",	"SHOD",	"SHOE",
"SHOT",	"SHOW",	"SHUN",	"SHUT",	"SICK",	"SIDE",	"SIFT",	"SIGH",
"SIGN",	"SILK",	"SILL",	"SILO",	"SILT",	"SINE",	"SING",	"SINK",
"SIRE",	"SITE",	"SITS",	"SITU",	"SKAT",	"SKEW",	"SKID",	"SKIM",
"SKIN",	"SKIT",	"SLAB",	"SLAM",	"SLAT",	"SLAY",	"SLED",	"SLEW",
"SLID",	"SLIM",	"SLIT",	"SLOB",	"SLOG",	"SLOT",	"SLOW",	"SLUG",
"SLUM",	"SLUR",	"SMOG",	"SMUG",	"SNAG",	"SNOB",	"SNOW",	"SNUB",

```
"SNUG", "SOAK", "SOAR", "SOCK", "SODA", "SOFA", "SOFT", "SOIL",  
"SOLD", "SOME", "SONG", "SOON", "SOOT", "SORE", "SORT", "SOUL",  
"SOUR", "SOWN", "STAB", "STAG", "STAN", "STAR", "STAY", "STEM",  
"STEW", "STIR", "STOW", "STUB", "STUN", "SUCH", "SUDS", "SUIT",  
"SULK", "SUMS", "SUNG", "SUNK", "SURE", "SURF", "SWAB", "SWAG",  
"SWAM", "SWAN", "SWAT", "SWAY", "SWIM", "SWUM", "TACK", "TACT",  
"TAIL", "TAKE", "TALE", "TALK", "TALL", "TANK", "TASK", "TATE",  
"TAUT", "TEAL", "TEAM", "TEAR", "TECH", "TEEM", "TEEN", "TEET",  
"TELL", "TEND", "TENT", "TERM", "TERN", "TESS", "TEST", "THAN",  
"THAT", "THEE", "THEM", "THEN", "THEY", "THIN", "THIS", "THUD",  
"THUG", "TICK", "TIDE", "TIDY", "TIED", "TIER", "TILE", "TILL",  
"TILT", "TIME", "TINA", "TINE", "TINT", "TINY", "TIRE", "TOAD",  
"TOGO", "TOIL", "TOLD", "TOLL", "TONE", "TONG", "TONY", "TOOK",  
"TOOL", "TOOT", "TORE", "TORN", "TOTE", "TOUR", "TOUT", "TOWN",  
"TRAG", "TRAM", "TRAY", "TREE", "TREK", "TRIG", "TRIM", "TRIO",  
"TROD", "TROT", "TROY", "TRUE", "TUBA", "TUBE", "TUCK", "TUFT",  
"TUNA", "TUNE", "TUNG", "TURF", "TURN", "TUSK", "TWIG", "TWIN",  
"TWIT", "ULAN", "UNIT", "URGE", "USED", "USER", "USES", "UTAH",  
"VAIL", "VAIN", "VALE", "VARY", "VASE", "VAST", "VEAL", "VEDA",  
"VEIL", "VEIN", "VEND", "VENT", "VERB", "VERY", "VETO", "VICE",  
"VIEW", "VINE", "VISE", "VOID", "VOLT", "VOTE", "WACK", "WADE",  
"WAGE", "WAIL", "WAIT", "WAKE", "WALE", "WALK", "WALL", "WALT",  
"WAND", "WANE", "WANG", "WANT", "WARD", "WARM", "WARN", "WART",  
"WASH", "WAST", "WATS", "WATT", "WAVE", "WAVY", "WAYS", "WEAK",  
"WEAL", "WEAN", "WEAR", "WEED", "WEEK", "WEIR", "WELD", "WELL",  
"WELT", "WENT", "WERE", "WERT", "WEST", "WHAM", "WHAT", "WHEE",  
"WHEN", "WHET", "WHOA", "WHOM", "WICK", "WIFE", "WILD", "WILL",  
"WIND", "WINE", "WING", "WINK", "WINO", "WIRE", "WISE", "WISH",  
"WITH", "WOLF", "WONT", "WOOD", "WOOL", "WORD", "WORE", "WORK",  
"WORM", "WORN", "WOVE", "WRIT", "WYNN", "YALE", "YANG", "YANK",  
"YARD", "YARN", "YAWL", "YAWN", "YEAH", "YEAR", "YELL", "YOGA",  
"YOKE" };
```

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru