КРИПТОГРАФИЯ И СТЕНОГРАФИЯ

ВЫПОЛНИЛА: ВАСИЛЬЕВА САРДААНА НИКОЛАЕВНА

СТУДЕНТКА ГР. ПКС-15

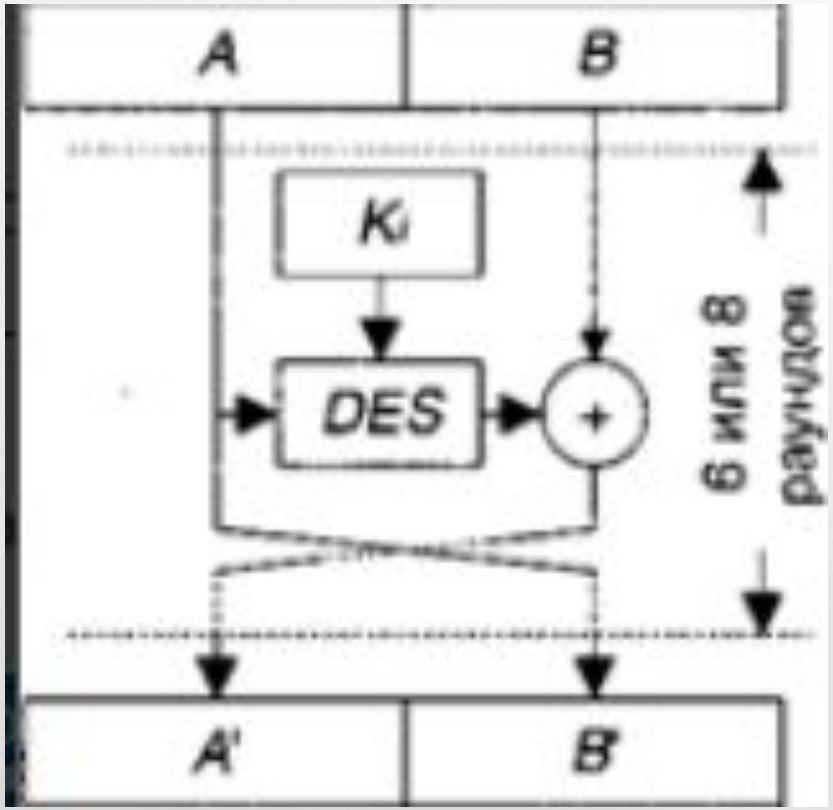
ЧТО ТАКОЕ КРИПТОГРАФИЯ И СТЕНОГРАФИЯ?

- **КРИПТОГРАФИЯ –** (ОТ ДР.-ГРЕЧ. ΚΡΥΠΤΌΣ — СКРЫТЫЙ И ΓΡΆΦΩ — ПИШУ) — НАУКА О МЕТОДАХ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ (НЕВОЗМОЖНОСТИ ПРОЧТЕНИЯ ИНФОРМАЦИИ ПОСТОРОННИМ), ЦЕЛОСТНОСТИ ДАННЫХ (НЕВОЗМОЖНОСТИ НЕЗАМЕТНОГО ИЗМЕНЕНИЯ ИНФОРМАЦИИ), АУТЕНТИФИКАЦИИ (ПРОВЕРКИ ПОДЛИННОСТИ АВТОРСТВА ИЛИ ИНЫХ СВОЙСТВ ОБЪЕКТА), А ТАКЖЕ НЕВОЗМОЖНОСТИ ОТКАЗА ОТ АВТОРСТВА.О

- **СТЕНОГРАФИЯ –** (ОТ ГРЕЧ. ΣΤΕΝΌΣ — УЗКИЙ, ТЕСНЫЙ И ΓΡΆΦΕΙΝ — ПИСАТЬ) — СПОСОБ ПИСЬМА ПОСРЕДСТВОМ ОСОБЫХ ЗНАКОВ И ЦЕЛОГО РЯДА СОКРАЩЕНИЙ, ДАЮЩИЙ ВОЗМОЖНОСТЬ БЫСТРО ЗАПИСЫВАТЬ УСТНУЮ РЕЧЬ[1].

- СКОРОСТЬ СТЕНОГРАФИЧЕСКОГО ПИСЬМА ПРЕВОСХОДИТ СКОРОСТЬ ОБЫЧНОГО В 4—7 РАЗ.

Криптографический алгоритм DEAL



Алгоритм DEAL разработан в 1998 г. известным криптоаналитиком Ларсом Кнудсеном. Ларе Кнудсен является автором большого числа криптоаналити-ческих исследований, описывающих различные виды атак на многие известные алгоритмы шифрования, в частности, на бывший тогда стандартом шифрования данных США алгоритм DES.

Название алгоритма DEAL произошло именно от DEA; по замыслу автора алгоритма, «DEAL» — это DEA (DES) с длинным блоком. Фактически DEAL — это вариант алгоритма DES с увеличенным размером блока и уве личенной длиной ключа. По своей структуре DEAL представляет собой сеть Фейстеля, в каждом раунде которой для преобразования субблока данных используется обычный алгоритм DES

Алгоритм шифрует данные 128-битными блоками с использованием трех фиксированных размеров ключей: 128, 192 и 256 битов. При использовании 256-битного ключа выполняется 8 раундов шифрования, для ключей остальных
размеров — 6 раундов.

В каждом раунде алгоритма выполняются следующие действия:

$$A_i = B_{i-1} \oplus DES_{Ki}(A_{i-1});$$
$$B_i = A_{i-1},$$

- / — номер текущего раунда;
- *Aj* и В,- — текущие значения левого и правого субблоков соответственно;
- *Ki* — ключ /-го раунда.

Процедура расширения ключа

Процедура расширения ключа предназначена для генерации 6 или 8 ключей *Ki* из исходного ключа шифрования. Процесс генерации ключей раундов незначительно различается в зависимости от размера ключа шифрования. Для 128-битных ключей расширение выполняется следующим образом

$$K_1 = DES_K(KI_1);$$
$$K_2 = DES_K(KI_2 \oplus K_1);$$
$$K_3 = DES_K(KI_1 \oplus C_1 \oplus K_2);$$
$$K_4 = DES_K(KI_2 \oplus C_2 \oplus K_3);$$
$$K_5 = DES_K(KI_1 \oplus C_4 \oplus K_4);$$
$$K_6 = DES_K(KI_2 \oplus C_8 \oplus K_5).$$

где:

- *К1П* — *п-й* 64-битный фрагмент исходного ключа шифрования;
- *Cj* — 64-битные константы, в которых бит *j* установлен в 1, а остальные биты обнулены;

ДОСТОИНСТВА И НЕДОСТАТКИ DEAL

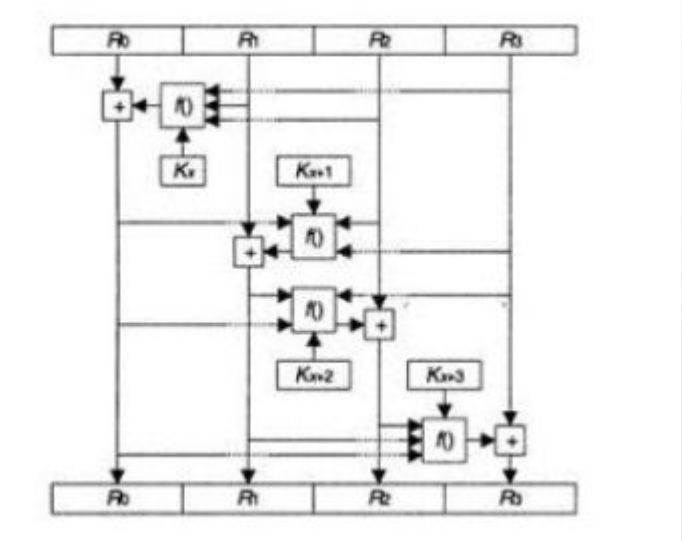
ДОСТОИНСТВА +

- АЛГОРИТМ DEAL ИМЕЕТ ЕДИНСТВЕННОЕ ЯРКО ВЫРАЖЕННОЕ ДОСТОИНСТВО— ЕГО МОЖНО РЕАЛИЗОВАТЬ С ИСПОЛЬЗОВАНИЕМ АППАРАТУРЫ ШИФРОВАНИЯ, РЕАЛИЗУЮЩЕЙ АЛГОРИТМ DES

НЕДОСТАТКИ -

- НЕСОМНЕННЫМ ЖЕ НЕДОСТАТКОМ АЛГОРИТМА ЯВЛЯЕТСЯ ЕГО ДОСТАТОЧНО НЕВЫСОКАЯ СКОРОСТЬ, КОТОРАЯ ОБСУЖДАЛАСЬ ВЫШЕ. КРОМЕ ТОГО, ИЗВЕСТНЫ ДВЕ КРИПТОАНА-ЛИТИЧЕСКИЕ РАБОТЫ, В КОТОРЫХ ДОКАЗАНА НЕДОСТАТОЧНАЯ КРИПТОСТОЙКОСТЬ АЛ ГОРИТМА DEAL.

Криптографический алгоритм RC2



Алгоритм шифрования RC2 был разработан в конце 1980-х гг. (в различных источниках указаны 1987 [395] и 1989 [224] гг.) Рональдом Ривестом, который, в частности, разработал алгоритм RC5, рассмотренный в *разд. 3.42*.
является собственностью компании RSA Data Security [390]; при этом известен тот факт, что разработку данного алгоритма инициировала и частично спонсировала фирма Lotus, которой требовался сильный (но не являющийся широко распространенным) алгоритм шифрования для последующего использования в программной системе Lotus Notes. Причем криптостойкость алгоритма должна была быть проверена Агентством Национальной Безопасности (АНБ) США. АНБ также внесло свой вклад в разработку алгоритма, предложив некоторые детали реализации, внедренные в алгоритм Ривестом

Структура алгоритма

Алгоритм является сетью Фейстеля, в нем выполняются 18 раундов преобразований. Причем раунды алгоритма делятся на 2 типа: смешивающие (mix) раунды и объединяющие (mesh) раунды. Общая структура алгоритма такова:

1. Выполняются 5 смешивающих раундов.
2. Выполняется 1 объединяющий раунд.
3. Выполняются 6 смешивающих раундов.
4. Выполняется 1 объединяющий раунд.
5. Выполняются 5 смешивающих раундов.

Расшифровывание

Расшифровывание выполняется по той же общей схеме, что и зашифровыва- ние. Однако при расшифровывании используются другие операции, выполняемые в смешивающем и объединяющем раундах.

$$R_i = R_i - K_n \bmod 2^{16};$$

где $n = R_{i-1 \bmod 4} \,\&\, 63$.

Криптографический алгоритм RC5

Алгоритм разработан известнейшим криптологом Рональдом Ривестом — одним из разработчиков асимметричной системы RSA и одним из основателей одноименной фирмы (RSA Data Security), которая, несомненно, является одним из мировых лидеров рынка средств криптографической защиты информации. Аббревиатура RC обозначает, по разным источникам, либо Rivest Cipher, либо Ron’s Code, т. е., в совокупности, «шифр Рона Ривеста» .

Аналогично предыдущим алгоритмам шифрования Рона Ривеста RC2 *(см. разд. 3.41)* и RC4 (является потоковым шифром, поэтому в данной книге не описан), алгоритм RC5 получил весьма широкое распространение

Структура алгоритма

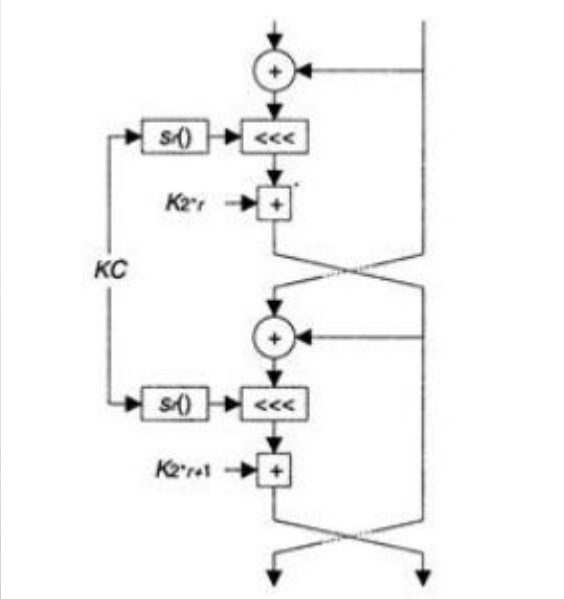
Аналогично, например, алгоритму SHARK *(см. разд. 3.50),* часть основных параметров алгоритма RC5 являются переменными. Как пишет автор алгоритма «RC5 — это несколько различных алгоритмов», поскольку, помимо секретного ключа, параметрами алгоритма являются следующие

? размер слова w (в битах); RC5 шифрует блоками по два слова; допустимыми значениями w являются 16, 32 или 64, причем 32 является рекомендуемым;

? количество раундов алгоритма *R* — в качестве значения допустимо любое целое число от 0 до 255 включительно;

? размер секретного ключа в байтах Ъ — любое целое значение от 0 до 255 включительно.

Автор предусмотрел и проблему совместимости реализаций RC5 с различными параметрами — каждое зашифрованное сообщение рекомендуется предварять заголовком, содержащим список значений основных параметров алгоритма — предполагается, что в этом случае для расшифровывания сообщения следует установить параметры из заголовка, после чего (при наличии корректного ключа) сообщение легко будет расшифровано.



Раунд алгоритма RC5

Криптографический алгоритм SEAL

SEAL (англ. ***S**oftware-optimized **E**ncryption **Al**gorithm*, программно-оптимизированный алгоритм шифрования) — симметричный поточный алгоритм шифрования данных, оптимизированный для программной реализации. Разработан в IBM Филом Рогэвеем (*англ.*) (англ. *Phil Rogaway*) и Доном Копперсмитом (англ. *Don Coppersmith*) в 1993 году. Алгоритм оптимизирован и рекомендован для 32-битных процессоров. Для работы ему требуется кэш-память на несколько килобайт и восемь 32-битовых регистров. Скорость шифрования — примерно 4 машинных такта на байт текста. Для кодирования и декодирования используется 160-битный ключ.

Чтобы избежать нежелательной потери скорости по причине медленных операций обработки ключа, SEAL предварительно выполняет с ним несколько преобразований, получая в результате три таблицы определенного размера. Непосредственно для шифрования и расшифрования текста вместо самого ключа используются эти таблицы.

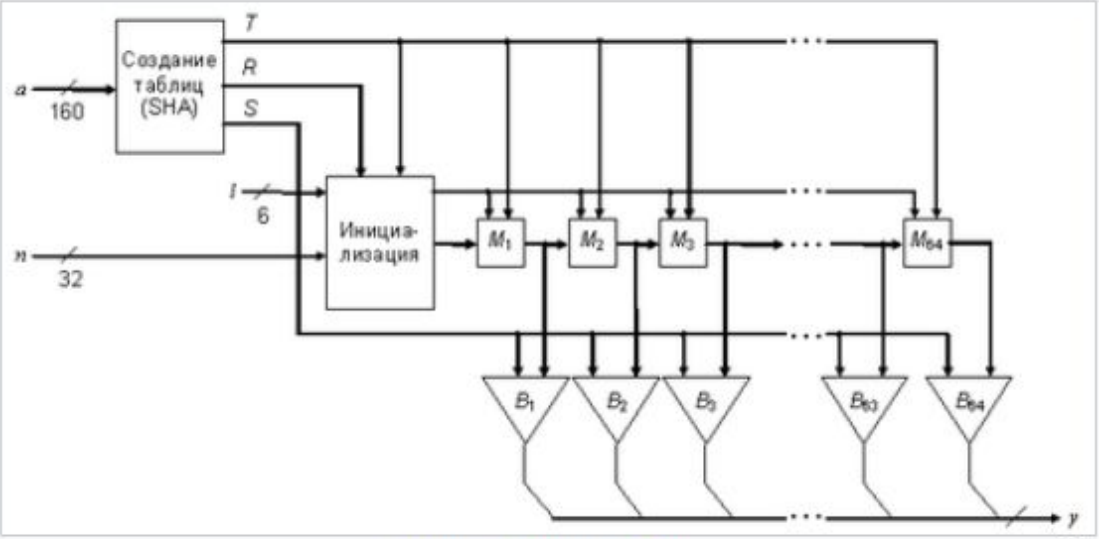


Схема алгоритма SEAL

Структура алгоритма

При описании алгоритма используются следующие операции и обозначения

- числа шестнадцатеричной системы счисления начинаются с символов **«0x»** и используют в записи кроме десятичных цифр символы ***«a»***, ***«b»***, ***«c»*** ***«d»***, ***«e»*** и ***«f»***, которые обозначают десятичные числа от ***10*** до ***15*** соответственно;
- под выражением $Y \ggg t$ следует понимать циклический сдвиг регистра Y вправо на t бит;
- под выражением $Y \lll t$ следует понимать циклический сдвиг регистра Y влево на t бит;
- операция $X \& Y$ означает побитовое логическое умножение (англ. *AND*) регистров X и Y;
- операция $X \vee Y$ означает побитовое логическое сложение (англ. *OR*) регистров X и Y;
- операция $X \oplus Y$ означает побитовое сложение по модулю 2 (англ. *XOR*) регистров X и Y;
- под $X \| Y$ следует понимать конкатенацию (англ. *Concatenation*) регистров X и Y;
- выражение ***odd (X)*** обозначает логическую функцию аргумента X, которая принимает значение ***ИСТИНА*** (англ. ***TRUE***) только, если X — чётное число.

Процесс шифрования состоит из большого числа итераций, каждая из которых завершается генерацией псевдослучайной функции. Количество пройденных итераций показывает счетчик ***l***. Все они подразделяются на несколько этапов с похожими операциями. На каждом этапе старшие 9 битов одного из регистров (***A***, ***B***, ***C*** или ***D***) используются в качестве указателя, по которому из таблицы ***T*** выбирается значение. Это значение складывается арифметически или поразрядно по модулю 2 (XOR) со следующим регистром (снова один из ***A***, ***B***, ***C*** или ***D***). Затем первый выбранный регистр преобразуется циклическим сдвигом вправо на 9 позиций. Далее либо значение второго регистра модифицируется сложением или XORом с содержимым первого (уже сдвинутым) и выполняется переход к следующему этапу, либо этот переход выполняется сразу. После 8 таких этапов значения ***A***, ***B***, ***C*** и ***D*** складываются (арифметически или XORом) с определенными словами из таблицы ***S*** и добавляются в ключевую последовательность ***y***. Завершающий этап итерации заключается в прибавлении к регистрам дополнительных 32-битных значений (***n1***, ***n2*** или ***n3***, ***n4***). Причем выбор конкретного значения зависит от четности номера данной итерации.

Свойства и практическое применение

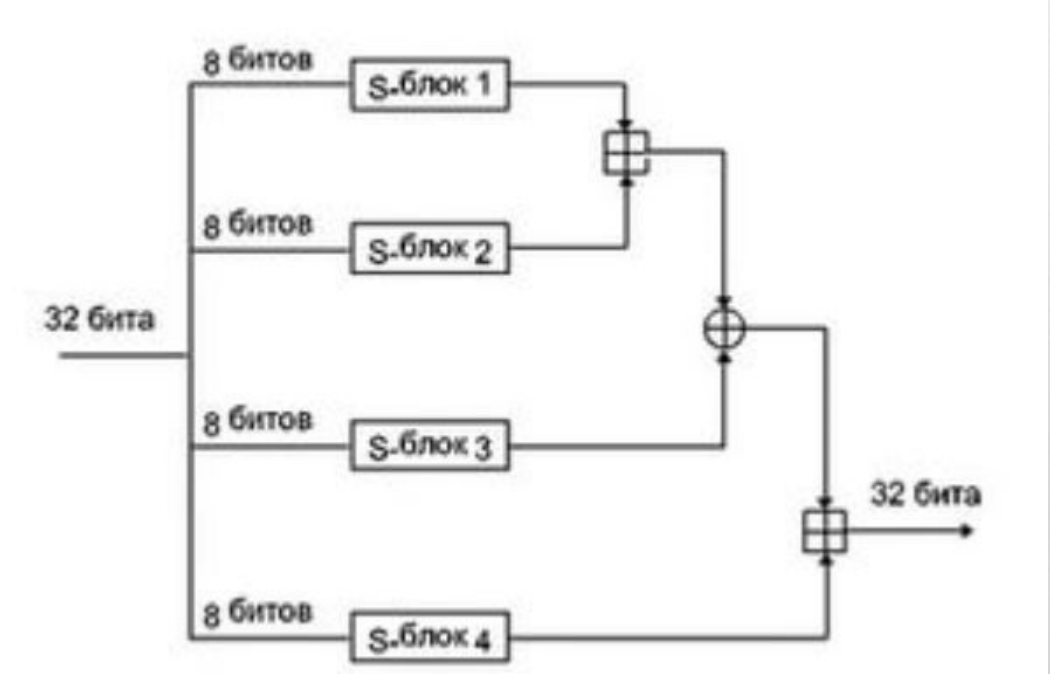
При разработке этого алгоритма главное внимание отводилось следующим свойствам и идеям:

- использование большой (примерно 2 Кбайта) таблицы ***T***, получаемой из большого 160-битного ключа;
- чередование арифметических операций (сложение и побитовый XOR);
- использование внутреннего состояния системы, которое явно не проявляется в потоке данных (значения *n1*, *n2*, *n3* и *n4*, которые изменяют регистры в конце каждой итерации);
- использование отличных друг от друга операций в зависимости от этапа итерации и её номера.

Для шифрования и расшифрования каждого байта текста шифр SEAL требует около четырех машинных тактов. Он работает со скоростью примерно 58 Мбит/с на 32-битном процессоре с тактовой частотой 50 МГц и является одним из самых быстрых шифров.

Криптографический алгоритм WAKE

Криптоалгоритм предложен в 1993 г. англичанином Д. Уилером из компьютерной лаборатории Кембриджского университета. – это аббревиатура словосочетания Word Auto Key Encryption (шифрование слов саморазворачивающимся ключом). Криптоалгоритм формирует гамму 32-разрядными словами в режиме обратной связи по шифротексту: предыдущее слово зашифрованного текста используется для порождения следующего слова гаммы. Главное достоинство – высокое быстродействие.



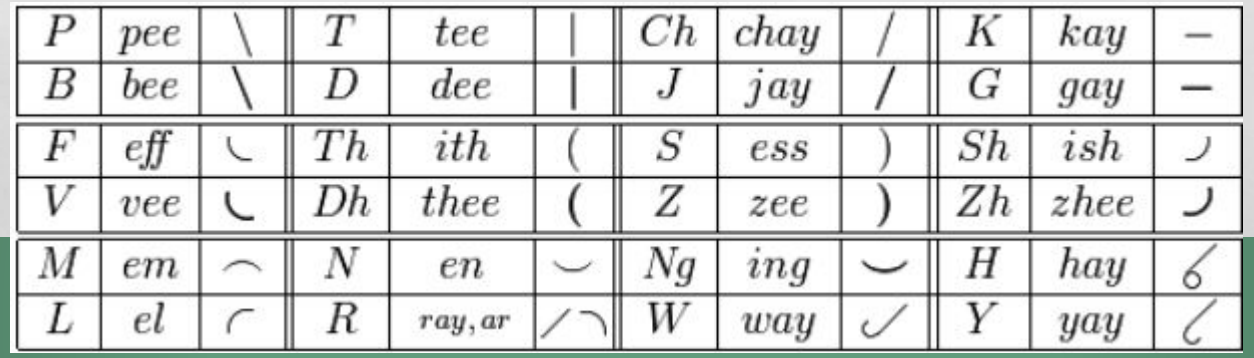
Достоинство

основное достоинство – его скорость. С точки же зрения криптографической стойкости он не столь хорош. В частности, алгоритм поддается атакам с подобранным шифротекстом.

Система Питмана

Одна из систем стенографии для английского языка, созданная англичанином сэром Айзеком Питманом (1813—1897) под названием «фонография». Первая публикация состоялась в 1837 году. Это фонетическая система, как и большинство систем скорописи; символы означают не буквы, а звуки речи. Ярким исключением является последовательная передача буквы *r*, даже при передаче звуков британской речи, в которой r зачастую не произносится. Возможная причина в том, что в середине XIX века в британском варианте английского ещё не начал выпадать этот звук. В 1996 году скоропись Питмана была самой популярной системой скорописи в Великобритании и второй по популярности в США.

Отличительной чертой скорописи является то, что звонкие и глухие звуки обозначаются одной и той же графемой, отличаясь только по толщине: толстые линии — звонкие согласные, тонкие линии — глухие согласные. Изначально для скоропись использовались перьевые ручки с мягкими перьями, в настоящее время этой скорописью обычно пишут карандашами.

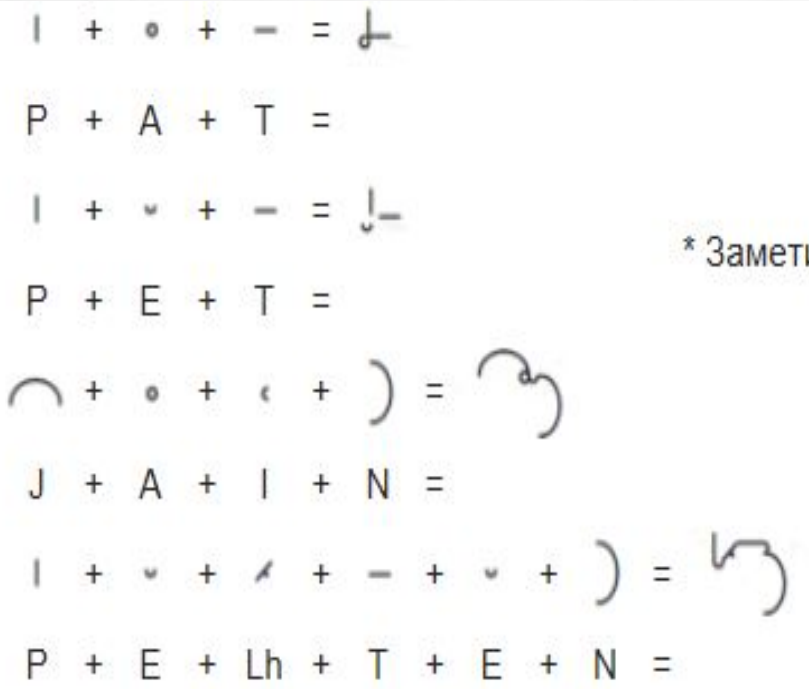


Система ДЮПЛОЙЕ

Система стенографии созданная Эмилем Дюплое в 1860 году для французского языка. С тех пор она была расширена и адаптирована для записи английского, немецкого, испанского, румынского, и чинукского.

Система Дюплойе классифицируется как геометрическая, буквенная, стенография и с написанием слева направо. Система Дюплойе была включена в Юникод с июня 2014 года, с выходом версии 7.0.

Соединения букв



* Заметим, что E обычно уходит влево P, кроме случая, когда должна соединиться с T.

Система Габельсбергера

Он издал получившие большое распространение в публике школьные прописи и *Mechan. Rechentafeln*, занимался изучением языков, мнемоникой, пазиграфией, криптографией, искусством дешифрировать письмена и изобретением скорописи. Все эти занятия помогали ему пролагать новые пути в стенографии. После введения в Баварии конституции и открытия парламентских дебатов он сделал стенографию главным предметом своих занятий. Он остановился на мысли, что видимые знаки, передающие звуки языка, должны быть приноровлены к организму и механизму человеческой речи. Эту основную мысль своей системы Габельсбергер постоянно проводил во всех усовершенствованиях её, которыми он занимался в продолжение 30 лет.

Ученики Габельсбергера основали «Габельсбергское главное стенографическое общество», которое, пользуясь оставшимися после Габельсбергера бумагами, переиздало его главное сочинение *Lehrgebäude der Stenographie* (Мюнхен, 1850).