Криптология и основные этапы её развития

Защита информации

Что защищаем?

Свойства информации:

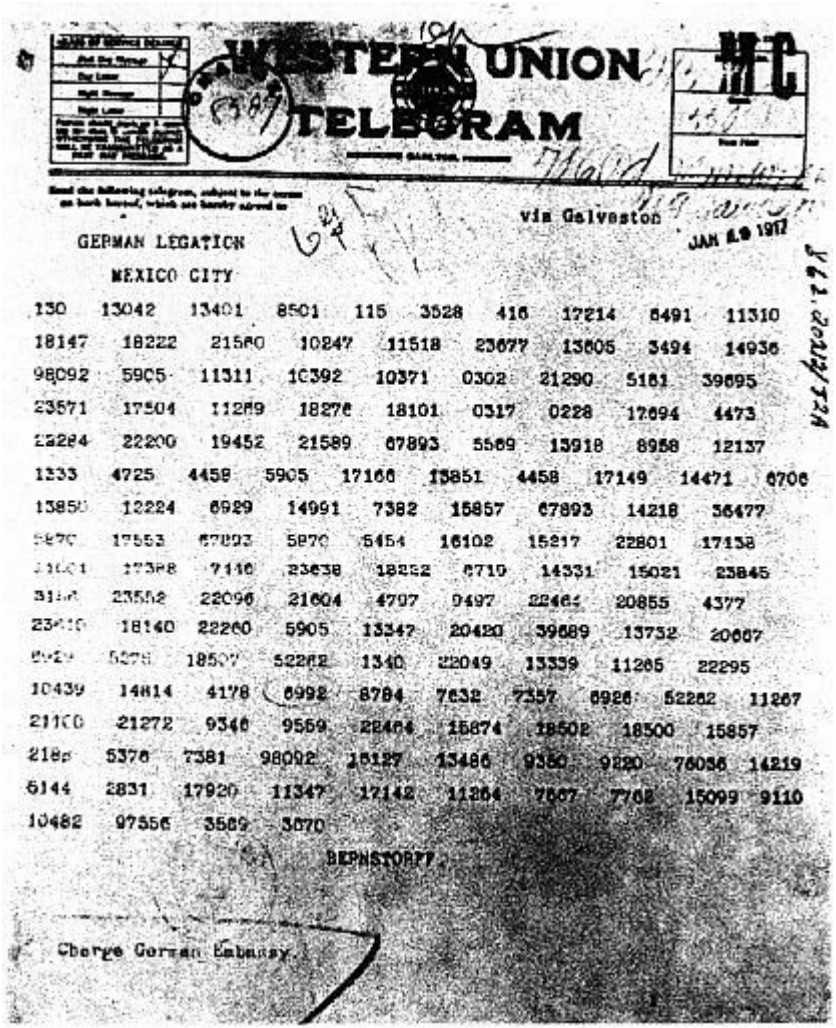
- конфиденциальность;
- целостность;
- доступность.

Способы защиты

- Физическая защита носителя информации
- Стеганографическая защита
- Криптографическая защита

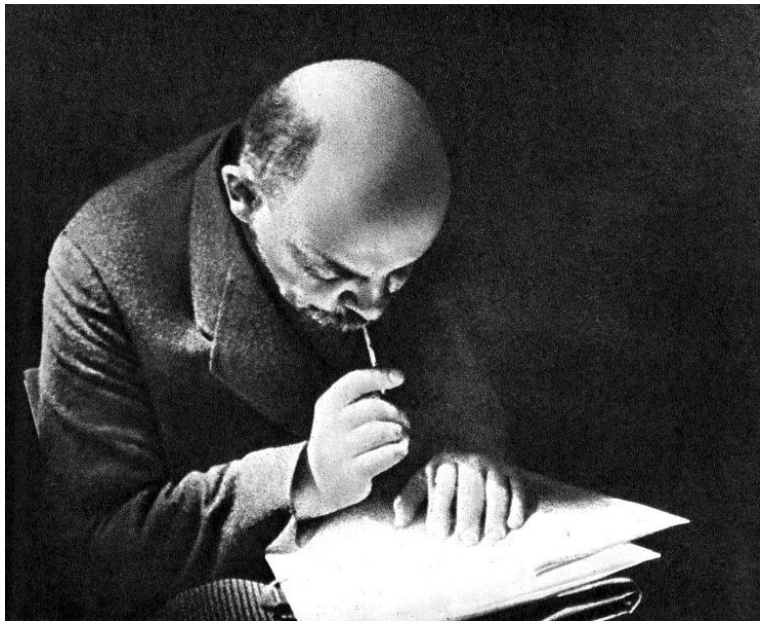
Крипторафическая защита

Исходный текст преобразуется путем замены, перестановки символов, групп символов так, что в результате получается нечитаемый и внешне бессмысленный текст (на рисунке — телеграмма Циммермана времен I Мировой войны).



Стеганографическая защита

Скрывается сам факт наличия информации, осуществляется тайная ее передача (микроточки, симпатические чернила, трафареты, запись на торце колоды карт и т. п.).



Письмо

- Предметное;
- пиктографическое;
- иероглифическое;
- слоговое;
- алфавитное.

Предметное письмо

Предметное письмо — это совокупность предметов, вещей, которые искусственно создавались или сочетались из природных вещей для передачи какой-либо информации.

Например, воткнутые у тропы ветки, зарубки на дереве, узоры из камней, информирующие идущих следом соплеменников о направлении движения, дым от костра как знак опасности, пучок стрел как символ объявления войны и др.

Пиктографическое письмо

ПИКТОГРАФИ́ЧЕСКОЕ ПИСЬМО́ (от лат. pictus — нарисованный и греч. grapho — пишу) (рисуночное письмо, пиктография), отображение общего содержания сообщения в виде рисунка или последовательности рисунков, обычно в целях запоминания. Известно с времен неолита.

В настоящее время: знаки дорожного движения, гербы, условные обозначения на вокзалах, в аэропортах, в магазинах, иконки компьютерных программ и т.п.

Иероглифическое письмо

Письмо, знаки которого представляют собой идеограммы, то есть обозначают целые понятия (несколько сотен символов).

Пример – китайские иероглифы, в древности иероглифическое письмо было распространено в Египте, Месопотамии, Древней Америке и др.

Слоговое письмо

Слоговое, или силлабическое письмо — вид фонетической письменности, знаки которой обозначают отдельные слоги (80-120 символов).

Примеры – японский язык(катакана и хирагана), логографическое китайское письмо, индийское письмо деванагари, клинопись.

त एत ऋषयो वेदं स्वं स्वं व्यस्यन्ननेकधा
शिष्यैः प्रशिष्यैस्तच्छिष्यैर्वेदास्ते शाखिनोऽभव

साधयित्वाजातशत्रोः स्वं राज्यं कितवैर्हृतम्
घातयित्वासतो राज्ञः कचस्पर्शक्षतायुषः

あいうえおかきくけこさしす

せそたちつてとなにぬねのは

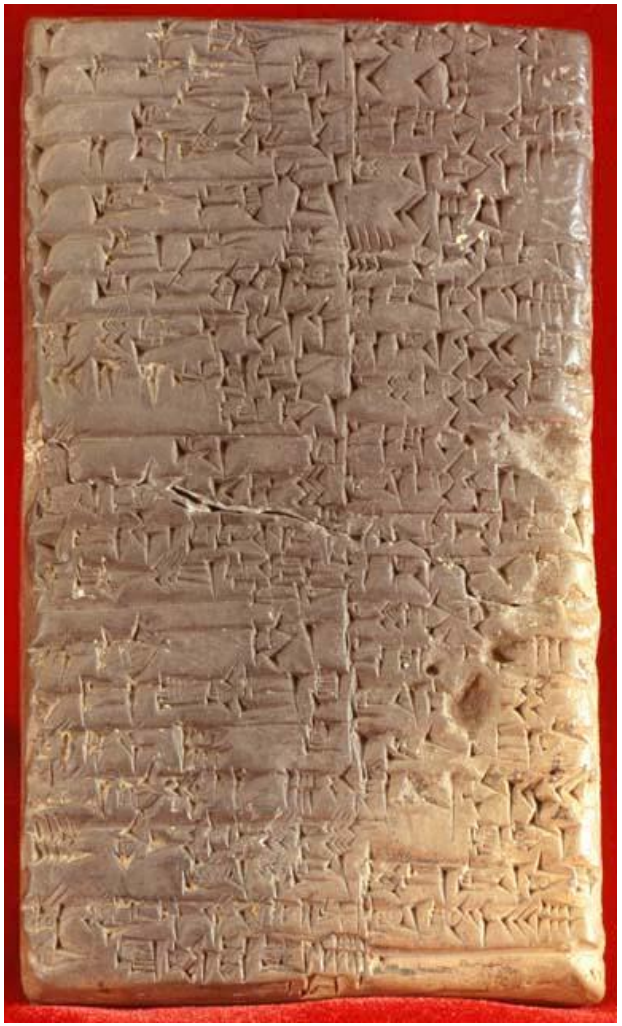
Алфавитное письмо

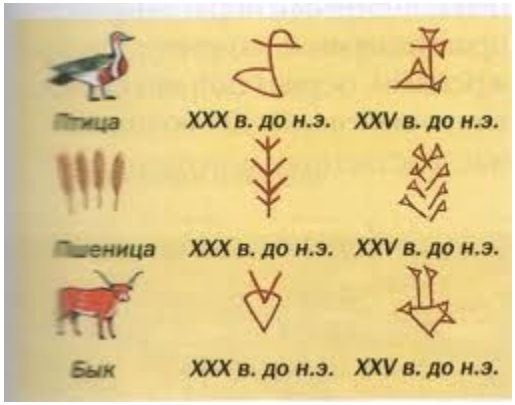
Алфавитное, или буквенно-звуковое письмо - тип письма, в котором каждый графический знак обозначает, как правило, отдельный звук (фонему). (15-40 символов).

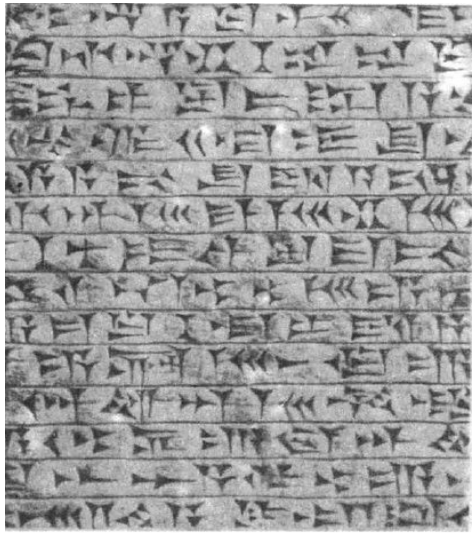
Примеры: кириллица, глаголица, латиница, еврейское квадратное, грузинское, армянское письмо.

Древний мир

Междуречье, IV тыс. до н.э. - 1 в. до н.э.




Птица
XXX в. до н.э.
XXV в. до н.э.
Пшеница
XXX в. до н.э.
XXV в. до н.э.
Бык
XXX в. до н.э.
XXV в. до н.э.



Древний Египет

Древний Египет
()

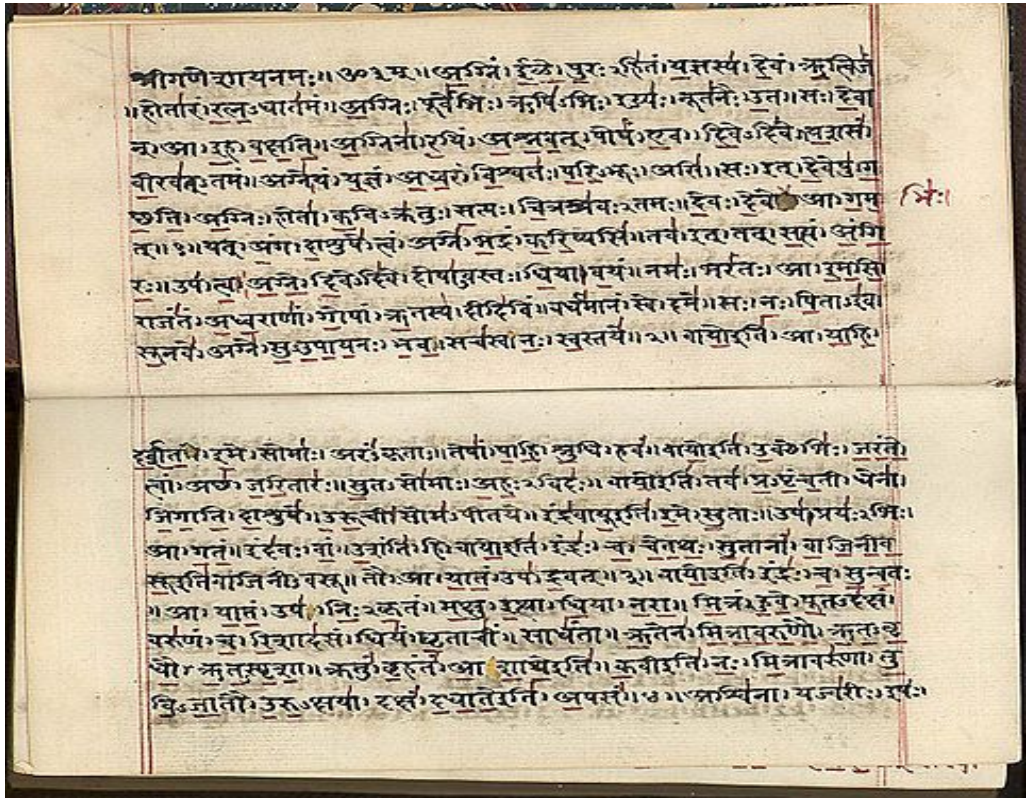
Палетка Нармера — один из древнейших памятников египетской письменности.

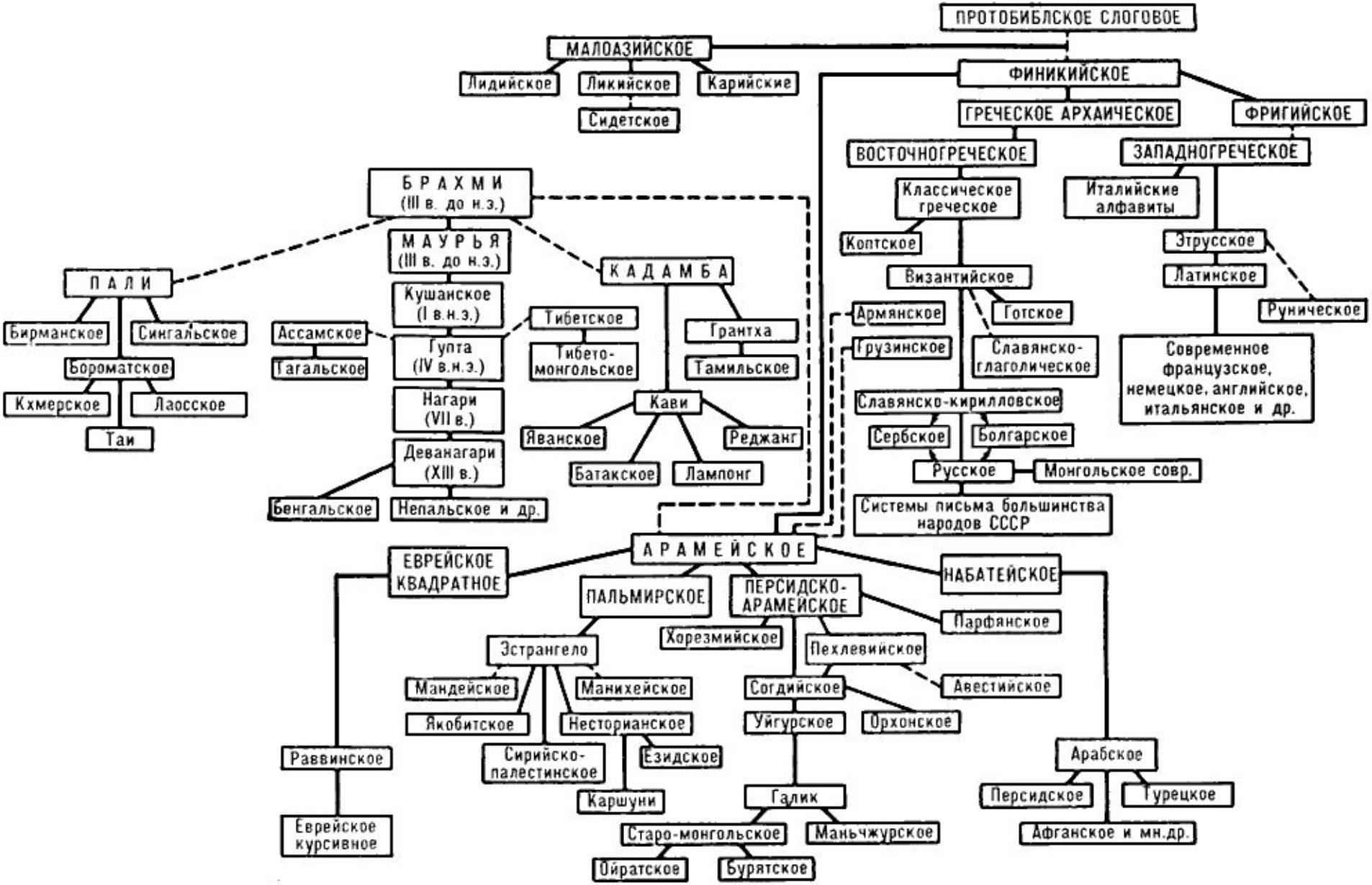
Древняя Индия

- Письменность долины Инда (2400-1800 гг. до н. э.) – не расшифрована.

Ареал распространения индской цивилизации.

- III в. до н. э. - III в. н.э. - брахми и кхароштхи (происходят от арамейского письма);
- III-VII в. н.э. - поздний брахми;
- с VII-сиддхам (от него происходит современное индийское письмо девнагари);




ПРОТОБИБЛСКОЕ СЛОГОВОЕ
МАЛОАЗИЙСКОЕ
Лидийское
Ликийское
Карийские
Сидетское
ФИНИКИЙСКОЕ
ГРЕЧЕСКОЕ АРХАИЧЕСКОЕ
ФРИГИЙСКОЕ
ВОСТОЧНОГРЕЧЕСКОЕ
ЗАПАДНОГРЕЧЕСКОЕ
Классическое греческое
Италийские алфавиты
Коптское
Византийское
Этрусское
Латинское
Армянское
Готское
Руническое
Грузинское
Славянско-глаголическое
Современное французское, немецкое, английское, итальянское и др.
Славянско-кирилловское
Сербское
Болгарское
Русское
Монгольское совр.
Системы письма большинства народов СССР
БРАХМИ (III в. до н.э.)
МАУРЬЯ (III в. до н.э.)
КАДАМБА
ПАЛИ
Кушанское (I в.н.э.)
Тибетское
Грантха
Ассамское
Гупта (IV в.н.э.)
Тибето-монгольское
Тамильское
Тагальское
Нагари (VII в.)
Кави
Бирманское
Сингальское
Яванское
Реджанг
Бороматское
Деванагари (XIII в.)
Батакское
Лампонг
Кхмерское
Лаосское
Бенгальское
Непальское и др.
Таи
АРАМЕЙСКОЕ
ЕВРЕЙСКОЕ КВАДРАТНОЕ
ПАЛЬМИРСКОЕ
ПЕРСИДСКО-АРАМЕЙСКОЕ
НАБАТЕЙСКОЕ
Парфянское
Хорезмийское
Пехлевийское
Эстрангело
Авестийское
Мандейское
Манихейское
Согдийское
Якобитское
Несторианское
Уйгурское
Орхонское
Раввинское
Сирийско-палестинское
Езидское
Арабское
Каршуни
Галик
Персидское
Турецкое
Еврейское курсивное
Старо-монгольское
Маньчжурское
Афганское и мн.др.
Ойратское
Бурятское

Древний Израиль

Атбаш (книга пророка Иеремии, VI в. до. н.э.).

Израиль в этот период находился под вавилонским владычеством.

Древняя Греция

Греческий алфавит (фонетическое письмо).

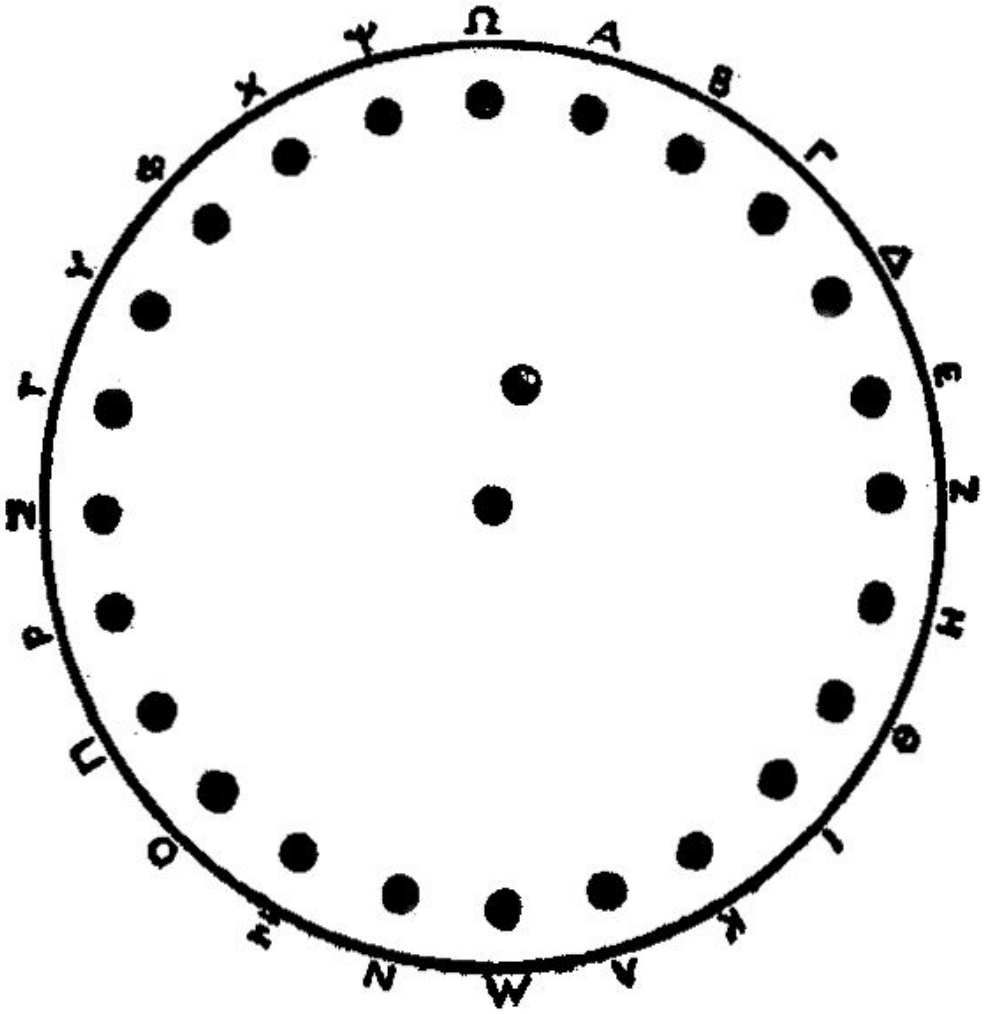
Сцитала (др. Спарта);

Диск Энея и линейка Энея;

Полибианский квадрат.

Сцитала (др. Спарта, V-VI вв. до н.э.)

Диск Энея (VI в. до н.э.)



Книжный шифр Энея

Квадрат Полибия (201-120 гг. до н.э.)

	1	2	3	4	5
1	А	Б	В	Г	Д
2	Е	Ж	З	И	К
3	Л	М	Н	О	П
4	Р	С	Т	У	Ф
5	Х	Ц	Ч	Ш	Щ
6	Ы	Ю	Я	-	-

Древний Рим

Шифр Цезаря (Гай Юлий Цезарь, 102-44 гг. до н.э.).

Шифр описан историком Гаем Светонием Транквиллом в труде «Жизнь 12-ти Цезарей» (75-160 гг. н.э.).