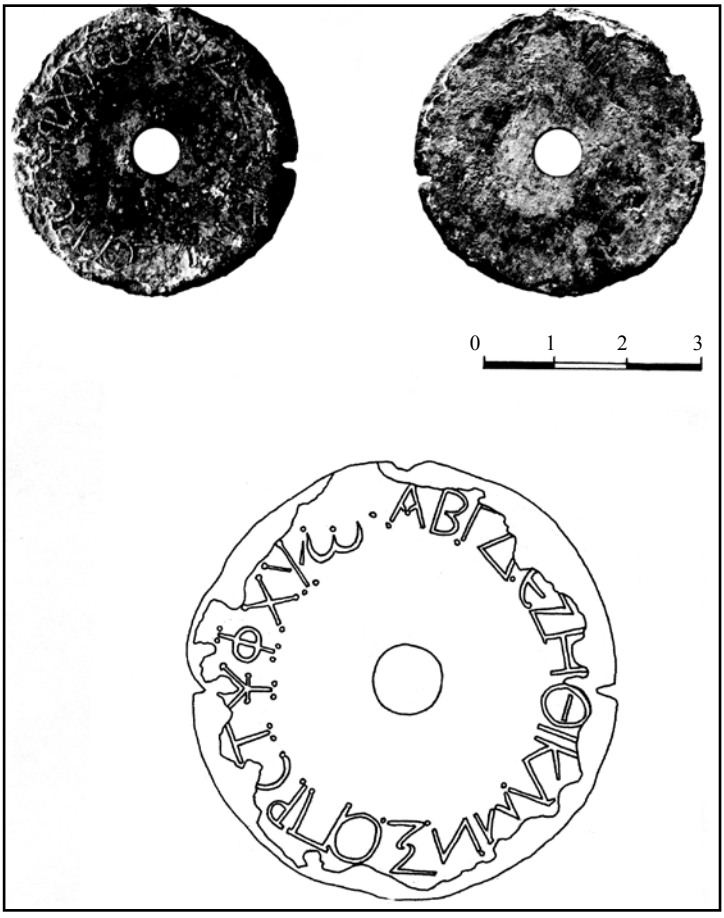
НАЦИОНАЛЕН ИСТОРИЧЕСКИ МУЗЕЙ – СОФИЯ
Известия, том XIV, 2004

ПРИСПОСОБЛЕНИЕ ЗА ШИФРОВАНЕ ОТ ВРЕМЕТО НА КЪСНАТА АНТИЧНОСТ

Николай Марков

Преди няколко години имах удоволствието да представя пред научната общественост един интересен предмет, наречен тогава от мен "гръцки абецедарий"[1] – название, неговорещо нищо за предназначението му. Тогава предложих няколко хипотетични виждания, но в крайна сметка предназначението на предмета остана неясно за мен. Днес, с натрупването на повече информация давам нова, надявам се достатъчно убедителна хипотеза, изясняваща този въпрос.

Какво представлява предметът? Това е кръгла бронзова пластина (дискче), върху чието лице, близо до периферията, е изписана гръцката азбука (Фиг. 1). Диаметъ-



Обр. 1. Външният диск от приспособлението за шифроване: а) лице; б) задна страна; в) рисунка

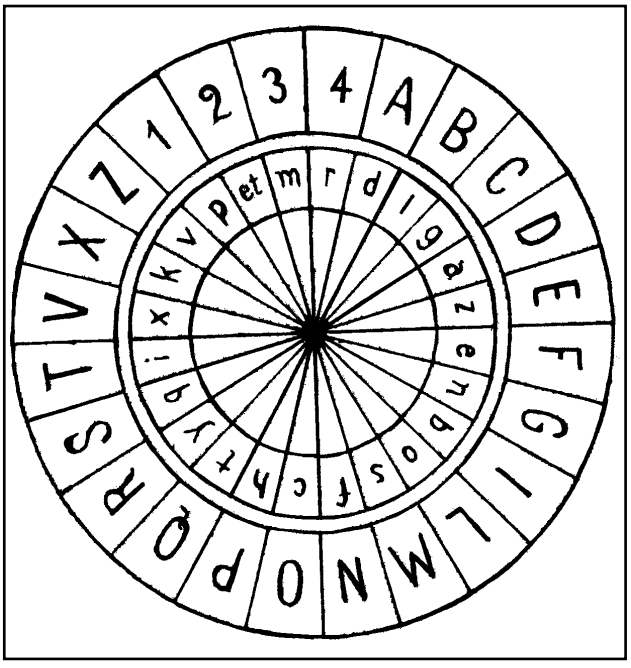
рът на дискчето е 39 мм, а дебелината му е около 2 мм. В средата е пробит кръгъл отвор, чийто диаметър е 6 мм. Двадесет и четирите букви, от A до ω, са гравирани с щихел. Средната им височина е около 4 мм. С начертанията си те стоят близо до гръцкото унциално писмо. При някои от буквите, с пунца са оформени точкови серифи. Между буквите A и ω е нанесена делителна точка. От ръба на периферията на дискчето до горните краища на буквите е оставено свободно поле от около 2 мм. В двата срещуположни края (при буквата Y и между H и Θ) ръбът на дискчето е леко зарязан. Гърбът му е равен и допълнително загладен. Като изключим силната деструкция на метала по периферията откъм лицето, засягаща на места и горните части на буквите, цялото дискче е обхванато от светло– до тъмнозелена патина.

Формата на предмета и някои негови същностни елементи –правилният отвор в средата му и зарязванията по периферията, подсказват, че той е имал някакво специфично предназначение.

Въз основа на някои характерни буквени очертания, при предходната си публикация датирах дискчето най-общо към II-IV век. Тази относително широка датировка дадох до голяма степен и поради неизвестните му произход и обстоятелства, при които то е намерено. Тук, без да предатирам този съхраняван в частна сбирка предмет, представям само новата си хипотеза за предназначението му.

Трябва да започна излагането ѝ с уговорката, че друг аналогичен предмет от античността не ми е известен. В замяна на това, от XV век насетне, до наши дни са достигнали немалко подобни екземпляри. Това са добре известните между професионалните шифровчици приспособления за шифроване и декодиране под названието Captain Midnight Decoder Badge[2] (Фиг. 2). За изобретател на това приспособление се смята изключително талантливият флорентинец Леон Батиста Алберти, а времето на създаването му е около 1466/67 г. Принципът на работата с това изключително по простотата си приспособление, съставено от два разположени един върху друг диска – външен, по-голям, неподвижен и вътрешен, подвижен – е основан на заместването на една буква с друга при предварително установена стъпка, позната естествено само на "посветените".

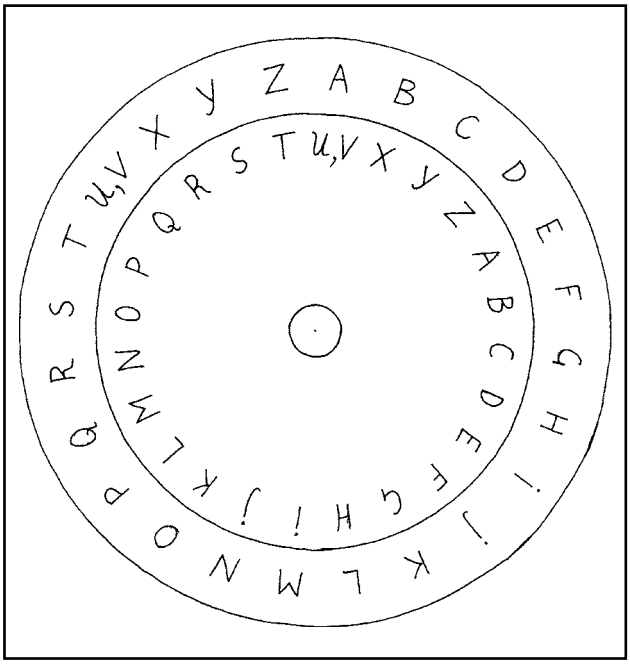
За да бъде разбран лесно ще си послужа с два примера, като работя върху предложената от мен схема, основана на латиницата. Според представите ми тя съответства по конструкцията си на използ-



Обр. 2. Шифровъчното приспособление на Алберти

ваното в античността приспособление, от което до нас е достигнал публикуваният тук диск (Фиг. 3). Как ще бъде шифрован прочутия израз на Цезар VENI VIDI VICI, който бил изписан по негово нареждане при Понтийския му триумф при разместване на буквите например с четири позиции? Ето резултатът: QAJE QEZE QEYE. А ако заменим, вътрешният диск с друг, с изписана гръцката азбука? Ще получим CAKE CEWE CEΨE. А ако сменим стъпката с три позиции? – RBKF RFAF RFZF. На практика комбинациите, които биха могли да бъдат получени при смяната на дисковете с буквените означения на двете основни азбуки –гръцката и латиницата – и комбинациите между двадесет и четирите им знака са напълно достатъчни, за да превърнат тази система на шифроване в достатъчна гаранция за опазване на тайната. Системата на кодиране, основана на работата с двата диска може да се усложни още, ако стъпката, през която се изместват буквите се променя в процеса на шифроването. Например, ако до десетата буква от текста тя е била 5, за следващата десетица тя може да се направи на 7 или на 12 и т. н. Дешифрирането на кодиран по тази система текст следвало обратния ред на заместването.

Имаме ли сведения за ползването на подобно шифроване от античността? Да, и това е известният шифър, с който си е служил Цезар при нужда. Ето какво четем у Гай Светоний Транквил в прочутото му съчинение Животът на цезарите, съставено в началото на II век: “Запазени са и негови [т. е. на Цезар] писма до Цицерон и до близките му по частни въпроси; ако в тях трябвало да съобщи нещо тайно, пишел го с шифър, тоест буквите били така разбъркани, че не образували никаква дума. За да се разшифрова и прочете, трябва да се замени всяка буква от азбуката с четвъртата след нея, тоест да се постави D вместо A и т. н....”[3]. Подобен е принципът и на шифроването използвано от Август. Отново източникът ни е Светоний: “Всеки път, когато употребявал шифър, [Август] пишел B вместо A, C вместо B и останалите букви по същия начин, а вместо Z – двойно AA”[4] На практика Август шифровал с изместване от 1 стъпка, като въвел и някои специфики. А ето какво пише за същата система на шифроване съвременникът на Светоний Авъл Гелий: “Запазени са писма на Г. Цезар до Г. Опиус и до Балбус Корнелиус, управлявали неговите имоти при отсъствията му. На някои



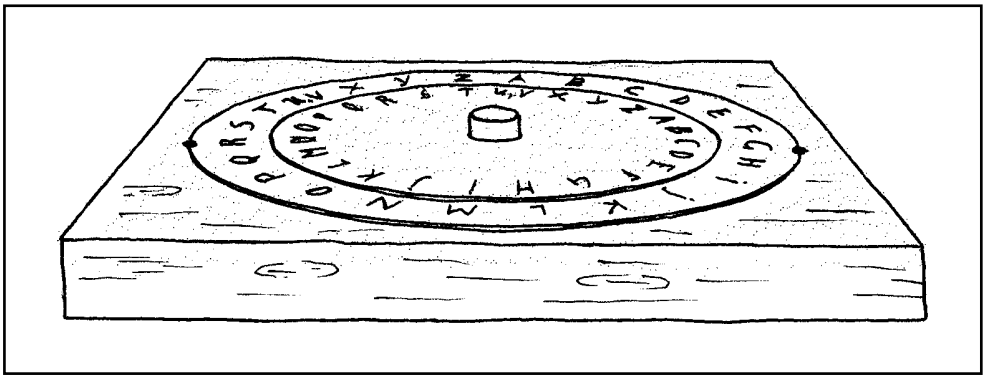
Обр. 3. Принципна възстановка на шифровъчно приспособление на латиница с изместване от четири позиции

места в тях се срещат отделни несвързани в срички букви, които не оформят думи и които изглеждат безредно разпръснати. Обаче между тях (Цезар и кореспондентите му) имало тайна уговорка за това как да разменят местата на буквите, така че при писане една буква да заема мястото и името на друга, но при четенето всяка да се върне на мястото си и да възвърне значението си. Като договорили използването на този таен начин на кореспонденция, те уточнили и кои букви с кои трябвало да бъдат заменяни. Граматикът Проб е изготвил старателно един коментар "За тайното значение на буквите в писмата на Г. Цезар".[5]

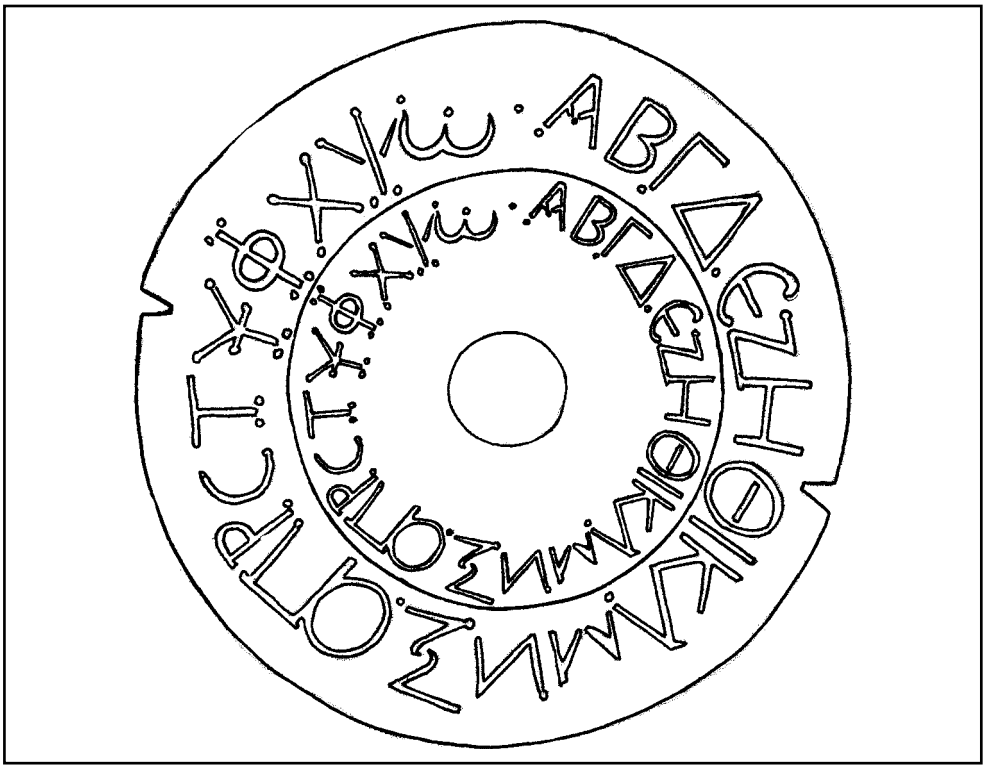
Как било монтирано проспособлението, чиято основна част представям тук? Първоначално дискчето било нанизвано на къса ос, закрепена най-вероятно в равна дървена основа. След това то било фиксирано неподвижно към нея чрез къси клинчета, прекарани в зарязванията по периферията му. Следвало нанизването към същата ос на по-малък, подобен по оформление диск, който обаче се въртял свободно около нея. Така приспособлението било готово за работа. На Фиг. 4 давам принципна възстановка според това описание, а на Фиг. 5 може да се види възстановката, която предлагам на представяното тук приспособление.

Новата находка или по-право преосмислянето ѝ, ми дава увереността да твърдя, че приписваното на Алберти изобретение за шифроване е всъщност много по-старо. Поне хилядолетие и половина преди времето на този талантлив флорентинец вече се ползвало подобно шифровъчно приспособление. Изглежда, че Алберти го познавал добре и всъщност само го усъвършенствал, макар и значително.

Представеният тук предмет е вероятно най-старото достигнало до наши дни шифровъчно и декодиращо приспособление в света[6]. За съжаление, липсата на вътрешния му диск не дава абсолютната сигурност, необходима за утвърждаването на хипотезата ми за неговото предназначение.



Обр. 4. Хипотетична възстановка на приспособлението в работно положение



Обр. 5. Хипотетична възстановка на представеното тук приспособление

БЕЛЕЖКИ

1. Бележки за новооткрит гръцки абецедарий от времето на късната античност. Археологически вести. 2. С., 2001. с. 20-22
2. Kahn, D. – "The Codebreakers". The Story of a Secret Writing. New-York. 1967, p. 127
3. Преводът на пасажа взимам от българското издание на Светоний –Дванадесетте цезари. С. 1983, с. 36
4. Пак там, с. 97. В българския превод с двойно АА е записано, че Август предавал буквата "КС". Тук съм представил съответствията според френското издание на Светоний на Ernest Flamarion в превод на De la Harpe.
5. A. Gelii –Noctium Atticarum. Liber XVII. Caput IX (Ed. M. Nisard. Paris. 1878, p. 703); в тази глава А. Гелий дава сведения и за други тайнописи, използвани през античността (напр. за прочутите лакедемонски σκυτάλη
6. Прочутите месопотамските плочки, намерени в Суза и датирани около 1500 г. пр. Хр., върху които с клинопис е записана формула за производство на керамична глазура са всъщност самия шифър (Kahn, D. – Opus cit., p. 75)

CIPHERING DEVICE FROM THE LATE ANTIQUITY PERIOD

Nikolay Markov

(Summary)

In this paper a round bronze plate (a small disc) is represented with the Greek alphabet running along the periphery of its face. The object has already been published by the author who now suggests a different function of the disc. Judging by the characteristic shaping of certain letters of the Greek alphabet, he dates the disc from the IInd – IIIrd centuries.

The author introduces arguments supporting his conclusion as to the object being most probably the earliest in the world ciphering/deciphering device that has come to us. Shown is its principal reconstruction and examples of its supposed usage are given. The idea is also supported by certain written information from the Antiquity concerning the cryptogram system, based on the simple replacing of letters. Evidently the functioning principle of the discussed device is of that type.