Лекция 1

Елементарни криптосистеми

1.1 Някои понятия в класическата криптография

Задачата за осъществяване на тайна комуникация по несигурен канал е първата криптографска задача, за която имаме исторически сведения. Ще опишем тази задача абстрактно, като се опитаме да отрзим достатъчно точно реалните ситуации, които възникват при предаване на данни с тайни съдържание.[1] Приемаме, че две партии, A и B (Алис и Боб) искат да обменят съобщения по несигурен канал, който се подслушва от опонент O (Оскар). Партиите A и B могат да бъдат физически лица, организации или устройства и обикновено се считат за добронамерени. Това означава, че те не се отклоняват от предписаните протоколи. Опонентът O е пасивен участник, който наблюдава обменените съобщения, но не може (засега) да ги модифицира. каналът е телефонна линия, компютърна мрежа или просто отрязък от време.

Да разгледаме следния прост сценарий на предаване на данни. A иска да изпрати съобщение на B,чието съдържание трябва да остане скрито за опонента O. Основният протокол, който A и B могат да използват, предполага наличието на *шифър* (или *криптосистема*). приемаме, че преди реалния обмен на данни A и B са се договорили за двойка параметризуеми алгоритми E_k и D_k, които се избират от някакви семейства $\mathcal{E}$ и $\mathcal{D}$ и се определят еднозначно от параметър k. Този параметър наричаме *ключ.* Приемаме, че всички потребители, включително и опонентът O, разполагат със семействата $\mathcal{E}$ и $\mathcal{D}$. Конкретният ключ k, използван при предаването на данните е неизвестен на O.

Нека конкретното съобщение, което A иска да предаде на B е m. Това съобщение наричаме още *открит текст.* преди предаването му A го преобразува с помощта на E_k, пресмятайки криптотекста

$$c = E(k, m)$$

и го изпраща на B. След получаването на криптотекста c потребителят B го *деш-*

[1]Понякога целта е да се скрие самото наличие на съобщение. Тази задача е обект на стеганографията.

[FIGURE]

ифрира с помощта на дешифриращия алгоритъм D_k, пресмятайки

$$m = D(k, c).$$

Алгоритмите (изображенията) E_k и D_k трябва да са избрани така, че опонентът O да не е в състояние да възстанови m от c без знанието на k. Описаният протокол е представенсхематично на фигурата по-долу.

Описаният сценарий е представен графично на схемата по долу.

Фиг 1. Конвенционална криптосистема

Понятието *криптосистема* е централно за криптографиыта. По-долу даваме една дефиниция, която описва основните черти на тези обекти без да е напълно удовлетворителна.

Дефиниция 1.1. *Криптосистема* (или *шифър* наричаме наредената петорка $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, където

(i) $\mathcal{P}$ е множеството от всички открити текстове;

(ii) $\mathcal{C}$ е множеството от всички криптотекстове;

(iii) $\mathcal{K}$ е крайно множество от всички възможни ключове;

(iv) $\mathcal{E}$ и $\mathcal{D}$ са множества от изображения, наричани съответно шифриращи и дешифриращи трансформации:

$$\mathcal{E} = \{E_k : \mathcal{P} \to \mathcal{C}, k \in \mathcal{K}\},$$

$$\mathcal{D} = \{E_k : \mathcal{C} \to \mathcal{P}, k \in \mathcal{K}\},$$

за които е изпълнено условието: за всеки ключ $k \in \mathcal{K}$ и за всяко съобщение $x \in \mathcal{P}$ е в сила

$$D_k(E_k(x)) = x.$$

Протоколът, към който се придържат A и B е следният. Най-напред те се уговарят да използват конкретна криптосистема и генерират по случаен начин ключ $k \in \mathcal{K}$. Можем да мислим, че k се създава от генератор на ключове и се предава по сигурен канал до A и B. Често този канал е най-скъпата, но и най-уязвимата част от криптосистемата. Ако A иска да изпрати съобщение $x = x_1 x_2 \ldots$, $x_i \in \mathcal{P}^*$, то тя пресмята $y_i = E_k(x_i)$, $i = 1, 2, \ldots$, и изпраща на B криптотекста $y = y_1 y_2 \ldots$. След получаване на криптотекста B дешифрира y, пресмятайки

$$x_i = D_k(y_i), i = 1, 2, \ldots.$$

разбира се, едно изисквана към системата е E_k да бъде инективна функция за всяко $k \in \mathcal{K}$, за да е има еднозначност на дешифрирането. Много често е изпълнено $\mathcal{P} = \mathcal{C}$. Тогава шифриращата и дешифриращата трансформации са просто пермутации.

1.2 Проста субституция

Един от най-ранните шифри се приписва на Юлий Цезар и носи неговото име – *шифър на Цезар*. Той се състои в заместване на всяка буква с буквата, намираща се три позиции по-назад в азбуката. Примерът по-долу илюстрира процедурата на шифриране:

```
i c a m e i s a w i c o n q u e r e d
L F D P H L V D Z L F R Q T X H U H G
```

Обратното преобразуване се състои в заместване на всяка буква със стоящата три позиции напред в азбуката. Строго погледнато това не е криптосистема, а една трансформация на $\mathcal{P}$. Не е трудно да се продължи тази идея. За целта е удобно буквите от английската азбука да се представят в числов вид. Тук използваме съответцтвието:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

което се счита за известно на всички страни, участващи в обмена на данни (включително O). Тогава описанота трансформация се изразява чрез

$$E\colon \left\{ \begin{array}{ccc} \{0,1,\ldots,25\} & \to & \{0,1,\ldots,25\} \\ x & \to & x+3 \pmod{26} \end{array} \right. .$$

Дешифрирането се задава е очевидно с $D(x) = E^{-1}(x) = x-3 \pmod{26}$. Можем да заменим константата 3 с произволен елемент от $\{0,1,\ldots,25\}$. Така стигаме до следния прост шифър, при който $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0,1,\ldots,25\}$, а шифрирането и дешифрирането се задават съответно с трансформациите:

$$\begin{array}{rcl} E_k(x) & = & x+k \pmod{26} \\ D_k(y) & = & y-k \pmod{26} \end{array}$$

Бихме могли да кажем, че $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$, където с $\mathbb{Z}_m$ означаваме както обикновено пръстена от остатъци по модул m, и че шифрирането и дешифрирането се състоят в прибавяне на ключа към откриния текст (съответно изваждане на ключа от криптотекста). Този шифър се обобщава като позволим $E_k(x)$ да бъде произволна обратима афинна трансформация в $\mathbb{Z}_{26}$. Сега отново $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, а множеството на ключовете се задава чрез

$$\mathcal{K} = \{k = (a,b)|\ a \in \mathbb{Z}_{26}^*, b \in \mathbb{Z}_{26}\},$$

Шифриращата и дешифриращата трансформации се задават съответно чрез

$$\begin{aligned} E_k(x) &= ax + b \pmod{26}, \\ D_k(y) &= a^{-1}y - a^{-1}b \pmod{26}. \end{aligned}$$

Така дефинирания шифър наричаме *афинен шифър*. За множеството от ключове имаме очевидно

$$|\mathcal{K}| = |\mathbb{Z}_{26}^*||\mathbb{Z}_{26}| = 12 \cdot 26 = 312,$$

което е прекалено малко за да позволява някаква практическата приложимост. Трансформацията на Цезар е пример на афинен шифър с ключ $k = (1, 3)$.

Да разгледаме афинен шифър с ключ $k = (7, 11)$. Тогава $E_k(x) = 7x + 11 \pmod{26}$, $D_k(y) = 15x + 17 \pmod{26}$. Шифрирането се извършва в съответствие с таблицата:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
11	18	25	6	13	20	1	8	15	22	3	10	17
L	S	Z	G	N	U	B	I	P	W	D	K	R

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
24	5	12	19	0	7	14	21	2	9	16	23	4
Y	F	M	T	A	H	O	V	C	J	Q	X	E

Така съобщението `complexity` се шифрира в `ZFRMKNQPOX`. При дешифриране можем да използваме същата таблица.

Можем да увеличим множеството от ключове като включим във $\mathcal{E}$ всички пермутации на $\mathcal{P}$. така нека $\mathcal{X} = \{A, B, \ldots, Z\}$ и

$$\mathcal{P} = \mathcal{C} = \mathcal{X}, \mathcal{K} = S_{\mathcal{X}}.$$

Тук $S_{\mathcal{X}}$ е симетричната група върху множеството $\mathcal{X}$. При избран ключ $\pi \in \mathcal{K}$ шифрирането и дешифрирането се задават чрез преобразуванията $E_\pi(x) = \pi(x)$ и $D_\pi(x) = \pi^{-1}(x)$. Такъв шифър наричаме *проста субституция*. Мощността на множеството от ключове е $26! = 403291461126605635584000000 \approx 4 \cdot 10^{26}$, което е достатъчно голямо дори от съвременна гледна точка. При такова огромно множество от ключове проблем представлява запомнянето на ключа. Съществуват различни методи за задаване на π. Един удобен начин е чрез *ключова фраза*. Таблицата, задаваща π, се конструира по следния начин: в първия ред се изпосва азбуката в естествения ѝ ред, а във втория – нейната пермутирана версия като се започва с клычовата фраза. Повторящите се букви (ако има такива) се игнорират; след свършване на ключа се дописва азбуката в естествения ѝ ред като се прескачат вече записаните букви. Да напишем пермутацията, получена от ключовата фраза `TURINGMACHINE`

A	B	C	D	E	F	G	H	I	J	K	L	M
T	U	R	I	N	G	M	A	C	H	E	B	D

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	J	K	L	O	P	Q	S	V	W	X	Y	Z

Съобщението `PERLHARBOUR` се шифрира в `KNOBATOUJSO`. При такава употреба ключовата фраза може да се мисли за ключ на описания шифър. Разбира се, с избора на ключова фраза ние силно ограничаваме множеството на използваните ключове, а с това и намаляваме сигурността на системата. По-нататък ще видим, че въпреки огромния брой ключове в общия случай, простата субституция е извънредно несигурна.

Простата субституция може да се използва с различни графични системи. Такава графична система е т.нар. *шифър на масоните.*

1.3 Шифър на **Playfair**

Шифърът, който излгаме по-долу представим е по същество субституционен. Той носи името на барон Plaifair of St. Andrews. [2]

При този шифър множеството на откритите текстове е множеството от всички наредени двойки от различни букви, т.е.

$$\mathcal{P} = \{A, \ldots, Z\} \times \{A, \ldots, Z\} \setminus \{(a, a) \mid a \in \{A, \ldots, Z\}.$$

Множеството на криптотекстовете съвпада с това на откритите текстове. Множеството от ключовете се състои от всички квадратни таблици 5×5, във всяка от които са подредени буквите от английската азбука без буквата `J`. При поява на `J` в открития текст тя се заменя с `I`, което не пречи на разбирането на съобщението. Един възможен ключ е, например

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

Шифрирането и дешифрирането се извършват с помощта на тази таблица в съотетствие със следните правила:

(1) Съобщението се разбива на двубуквени блокове, всеки от които съдържа *различни* букви. Общата дължина на съобщението е четна. Ако тези две свойства не са в сила за избраното съобщение, то то се модифицира. Например, може да бъде допусната ирелевантна правописна грешка (непроменяща смисъла) или се добавя нискочестотна буква в края за получаване на четна дължина на съобщението. Така `CRYPTOGRAPHY` съобщение, удовлетворяващо изискванията, поставени за открит текст. След разбиването му на блокове получаваме `CR YP TO GR AP HY`,

[2] Всъщност автор на шифъра е е английския физик Charles Wheatstone (1802–1875). През 1854 г. последният демонстрирал пред подсекретаря на Форин офис шифъра, известен днес като Playfair. За да изтъкне простотата на на шифъра той отбелязал по време на демонстрацията, че три от всеки четири деца от съседното училище биха могли да бъдат обучени да шифрират в рамките на няколко минути. На това получил сухия отговор “that’s very possible, but you could never teach it attachês”.

Съобщения като CHESTER или MISSISSIPPI нарушават тези условия. В първия случай можем да добавим буквата X в края на думата, получавайки

CH ES TE RX.

Във втория случай разделяме идентични съседни букви с разделителя Z, получавайки

MI SZ SI SZ SI PZ PI.

(2) След като сме осигурили всеки блок на съобщението да съдържа две различни букви, пристъпваме към шифрирането. То се извършва поблоково. Ако двете букви на един блок са в различни редове и различни стълбове на използваната таблица, о се използва т.нар. "правило на правоъгълника". Буквите на блока задават в таблицата правоъгълник със трани успоредно на редовете и стълбовете ѝ. Така всеки блок съдържа върховете на диагонал в еднозначно определен правоъгълник. Криптотекстът за този блок е другият диагонал в правоъгълника. Така в горната таблица блокът WR определя правоъгълника WSRU и се изобразява в другия диагонал SU. При това първите буква от съответните блокове открит текст и криптотекст са в един и същи ред. По това правило имаме

$$\texttt{RW} \to \texttt{US},\ \texttt{SU} \to \texttt{WR},\ \texttt{XB} \to \texttt{HQ},\ \texttt{TL} \to \texttt{ER}.$$

Ако буквите на един блок са в един и същи ред (съответно един и същи стълб), шифрирания блок се получава чрез изместване на една позиция вдясно (съответно една позиция надолу). Това се изместване е циклично, т.е. считаме че стълбът, намиращ се вдясно от петия е първият, както и че редът под петия ред е първият ред. Така PL се изобразява в UR, TR – в BH, GE – в ET, EF – в VE, CK – в NY.

Да шифрираме откриния текст CRYPTOGRAPHY като използваме ключа (таблицата), даден по-горе. Очевидно имаме

$$\texttt{CR}\to\texttt{HI},\quad \texttt{YP}\to\texttt{DI},\quad \texttt{TO}\to\texttt{NG},\quad \texttt{GR}\to\texttt{TU},\quad \texttt{AP}\to\texttt{OA},\quad \texttt{HY}\to\texttt{CS}.$$

Така криптотекстът, съотвецтващ на CRYPTOGRAPHY е HIDINGTUOACS.

(3) Дешифрирането е аналогично на шифрирането. Ако буквите на един блок от криптотекста са в различни редове и различни стълбове, то ние ги заменяме с буквите от другия диагонал на еднозначно определения от тях правоъгълник. Ако буквите на блока са в един ред (един стълб), то извършваме цикличен шифт на една позиция вляво (нагоре).

Да отбележим, че цикличното преместване на цели редове или стълбове задава ключ (таблица), еквивалентен на изходния. Лесно се проверява, че таблицата

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

шифрира откритите текстове по същия начин както таблицата на стр. 5.

Шифърът, които описахме, допуска обобщение: може да се зададе друг начин за образуване на двойките букви в открития текст, таблицата 5×5 може да бъде заменена с таблица с други размери и пр. Тъй като точният ѝ вид на ключовата таблица се запомня трудно, можем да фиксираме правило, по което тя се образува. Например, можем да изберем клычова дума с произволна дължина, в която никои две букви не са идентични. Започваме запълването на таблицата с тази дума (отляво надясно и отгоре надолы), а след това допълваме и с останалите букви в естествения им ред. Така ключовата дума `CRYPTOENIGMA` ни дава таблицата

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

Избирането на клычовата таблица по това правило намалява множеството на допустимите ключове и намалява сигурността на системата.

1.4 Шифър на **L. Hill**

При проста субституция всяка буква от открития текст се заменя с фиксирана буква от криптотекста като правилото за замяна зависи от ключа. Таква шифри се наричат *моноалфабетни*. При тях честотите на символите от открития текст се запазват в криптотекста, което ги прави уязвими на атаки, базирани на статистически анализ. Шифърът на Plaifair с е състои в замяна на двойка букви от открития текст (започваща в нечетна позиция) с фиксирана двойка букви, като съответствието се определя от ключовата таблица. Сега прилагането на статистически методи се затруднява от това, че статистигата на двойките букви няма толкова ясно изразени максимуми, а и не всяка двоика от букви се шифрира винаги в една и съща двойка. Продължавайки по този начин можем да мислим за шифър, при който последователните m-орки от букви се заменят с фиксирани m-орка над същата азбука. Шифърът на Л. Хил [26] който ще опишем, реализира тази идея. Той е важен в теоретичен план и е многомерно обобщение на афинния шифър. Идеята е да се преобразуват наведнъж m символа като използваме линейна трансформация на вектор с m компоненти.

Нека $m \geq 2$ е фиксирано естествено число и нека $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$. Множеството на ключовете $\mathcal{K}$ е множеството на всички обратими $m \times m$ матрици над $\mathbb{Z}_{26}$. Шифрирането и дешифрирането се задават съответно чрзе трансформациите

$$\begin{aligned} E_K(\boldsymbol{x}) &= \boldsymbol{x}K \\ D_K(\boldsymbol{y}) &= \boldsymbol{y}K^{-1}. \end{aligned}$$

Ще отбележим, че една матрица $K = (k_{ij})_{m \times m}$, $k_{ij} \in \mathbb{Z}_{26}$, е обратима точно тогва когат детерминантата ѝ е обратим елемент в $\mathbb{Z}_{26}$, т.е. $(\det K, 26) = 1$. Обратната матрица може да се пресметне по известните методи за намиране на обратна матрица над поле. например, ако $\det K$ е обратим елемент в $\mathbb{Z}_{26}$, то

$$K^{-1} = \frac{1}{\det K}\left((-1)^{i+j}K_{ji}\right)_{m\times m}.$$

Пример 1.2. В този пример илюстрираме шифриране и дешифриране с шифър на Hill с $m = 3$ и с ключ матрицата

$$K = \begin{pmatrix} 9 & 5 & 0 \\ 0 & 1 & 3 \\ 5 & 18 & 2 \end{pmatrix}$$

Най-напред преобразуваме[3] съобщението `london`, във вектор над $\mathbb{Z}_26$:

$$\texttt{london} \;\to\; (11, 14, 13, 3, 14, 13).$$

Разбиваме получената шесторка на два блока с дължина 3, всеки от които шифрираме поотделно. Така получаваме:

$$(11, 4, 13)\begin{pmatrix} 9 & 5 & 0 \\ 0 & 1 & 3 \\ 5 & 18 & 2 \end{pmatrix} = (8, 17, 6) \;\to\; \texttt{ISQ}.$$

$$(3, 14, 13)\begin{pmatrix} 9 & 5 & 0 \\ 0 & 1 & 3 \\ 5 & 18 & 2 \end{pmatrix} = (14, 3, 6) \;\to\; \texttt{ODQ}.$$

Така `london`$\to$ISQODQ.

За да дешифрираме се нуждаем от обратната матрица K^{-1}. Тя съществува, тъй като $\det K = -3 = 23$. Сега пресмятаме

$$K^{-1} = -\frac{1}{3}\left(\begin{array}{ccc} \begin{vmatrix} 1 & 3 \\ 18 & 2 \end{vmatrix} & -\begin{vmatrix} 5 & 0 \\ 18 & 2 \end{vmatrix} & \begin{vmatrix} 5 & 0 \\ 1 & 3 \end{vmatrix} \\ -\begin{vmatrix} 0 & 3 \\ 5 & 12 \end{vmatrix} & \begin{vmatrix} 9 & 0 \\ 5 & 2 \end{vmatrix} & -\begin{vmatrix} 9 & 0 \\ 0 & 3 \end{vmatrix}) \\ \begin{vmatrix} 0 & 1 \\ 5 & 18 \end{vmatrix} & -\begin{vmatrix} 9 & 5 \\ 5 & 18 \end{vmatrix} & \begin{vmatrix} 9 & 5 \\ 0 & 1 \end{vmatrix} \end{array}\right) = \begin{pmatrix} 0 & 12 & 21 \\ 21 & 10 & 9 \\ 19 & 11 & 23 \end{pmatrix}.$$

Криптотекстът е `ISQODQ`$\to (8, 17, 16, 14, 3, 16)$ и дешифрирането се състои в умножение с K^{-1}:

$$(8, 17, 16)\begin{pmatrix} 0 & 12 & 21 \\ 21 & 20 & 9 \\ 19 & 11 & 23 \end{pmatrix} = (11, 14, 3) \;\to\; \texttt{lon}.$$

$$(14, 3, 16)\begin{pmatrix} 0 & 12 & 21 \\ 21 & 20 & 9 \\ 19 & 11 & 23 \end{pmatrix} = (3, 14, 13) \;\to\; \texttt{don}.$$

[3]Както навсякъде в тази глава, където се налага пребразуване на английски текст в числов вид, използваме кодирането $A \to 0$, $B \to 1$, $C \to 2$, ..., $Z \to 25$.

1.5 Шифър на **Vigenère**

Следващият шифър предшества исторически шифъра на Хил, но може да бъде разглеждан като негов специален случай. Тава е един от най-старите и може би най-популярният *полиалфабетен шифър*. Той носи името на френския криптограф Blaise Vigenère (1523-1596). Ще опишем този шифър с един пример, след което ще дадем и формално описание. Буквите на английската азбука са наредни в т.нар. квадрат на Vigenère [4] по указания по долу начин. Кавадратът на Vigenére се използва както при шифриране, така и при дешифриране Всеки стълб на таблицата се разглежда като транслационен шифър с ключове съответно $0, 1, \ldots, 25$. Редовете се асоциират с открития текст, а стълбовете с ключа. Например при шифриране на открития текст `cryptography` с ключа `RADIO` най-напред вземаме буквата, намираща се в ред `c` и стълб `R`, след това буквата в ред `r` и стълб `A` и т.н.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

[4] По-правилно е да се нарича квадрат на Trithemius, който първи е описал тази таблица (recta transpositionis tabula). Johannes Heidenberg aus Trittenheim, наречен Trithemius (1462–1516), е монах от бенедектинското абатство в Trittenheim an der Mosel. Той е автор на една от първите книги по криптография Polygraphiae.

Получаваме криптотекста `TRBXHFGUIDYY`:

```
c r y p t o g r a p h y
R A D I O R A D I O R A

T R B X H F G U I D Y Y
```

При дешифриране процедурата е следната - тъсим реда, който има буквата `T` в стълба, индексиран с `R`. Така намираме `c` и продължаваме по същия начин до пълното дешифриране. Ако откритият текст е по-дълъг от ключовата дума, то ние я повтаряме многократно. Така в горния пример ключовата дума `RADIO`, приложена към текст от 12 букви приема вида `RADIORADIORA`.

Описаната процедура може да бъде използвана и с други квадрати, най-известен от които е квадратът на Beaufort. [5]

Формално шифърът на Vigenère може да бъде описан така. Нека $m > 1$ е фиксирано естествено число. Нека по-нататък $\mathcal{P} = \mathcal{C} = \{0, 1, \ldots, 25\}^*$ (не е много удобно да пишем $(\mathbb{Z}_{26}^*)^*$), а $\mathcal{K} = \{0, 1, \ldots, 25\}^m$. При зададен открит текст $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1})$ и избран ключ $\boldsymbol{k}k = (k_0, k_1, \ldots, k_{m-1}$ шифрирането се задава чрез $E_{\boldsymbol{k}}(\boldsymbol{x}) = (y_0, y_1, \ldots, y_{n-1})$, където $y_i = x_i + k_{i \mod m} \pmod{26}$. За дешифрирането очевидно имаме $D_k(\boldsymbol{y}) = (z_0, z_1, \ldots, z_{n-1})$, където $z_i = y_i - k_{i \mod m} \pmod{26}$.

Ясно е, че и при шифъра на Хил и при този на Vigenére става въпрос за афинни трансформации на m-мерни вектори над $\mathbb{Z}_{26}$. Нека $\mathcal{M}_m(\mathbb{Z}_{26})$ е множеството на обратимите $m \times m$ матрици на $\mathbb{Z}_{26}$ и да положим

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m,\ \mathcal{K} = \mathcal{M}_m(\mathbb{Z}_{26}) \times \mathbb{Z}_{26}^m.$$

шифрирането и дешифрирането са задаени чрез:

$$E_{(K,\boldsymbol{k})}(\boldsymbol{x}) = \boldsymbol{x}K + \boldsymbol{k}, \quad D_{(K,\boldsymbol{k})}(\boldsymbol{y}) = \boldsymbol{y}K^{-1} - \boldsymbol{k}K^{-1}.$$

Това обобщава по естествен начин шифъра на Хил. В случая $m = 1$ получаваме афинния шифър, а при $\boldsymbol{k} = \boldsymbol{0}$ – класическия шифъна Хил. Шифърът на Vigenére получаваме $K = I_m$, къдети I_m е единичната матрица от ред m.

При практическото използване на шифрите на Vigenére и Хил дължината на ключа е неизвестна за опонента и може да се счита за част от ключа. Това води до трудности при криптанализа, които не са решени по удовлетворителен начин до средата на XIX век.

1.6 Пермутационни шифри

Обща черта на шифрите, разгледани дотук, е замяната на буква или група от букви с друга буква или друга група от букви по определено правило. Друг подход при създаването на шифър е да запазим непроменени символите от откриция текст и да променим позициите им. [6] а дефиниция на общ пермутационен шифър е следната.

[5] Носи името на адмирал сър Francis Beaufort, създател и на скала за измерване на скоростите на ветровете носеща неговото име.

[6] Пермутационните шифри се споменават за пръв път при Giovanni Porta (ок. 1563 г.)