3 Encryption Steps: Simple Substitution

Among the encryption steps we find prominently two large classes: substitution and transposition. They are both special cases of the most general encryption step $V^{(n)} \dashrightarrow W^{(m)}$. We shall start by looking at several kinds of substitution and turn our attention to transposition in Chapter 6 .

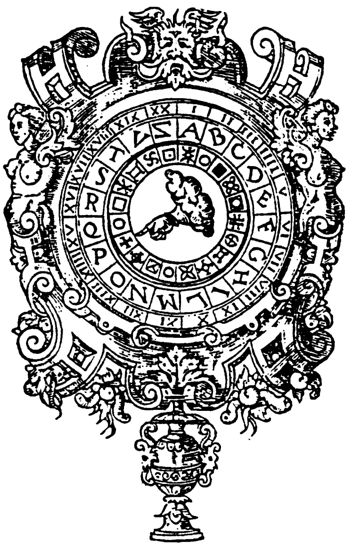
A simple substitution (German *Tauschverfahren* or *Ersatzverfahren*) is a substitution with monographic encryption steps $\chi_i \in M$,

$$\chi_i : V^{(1)} \dashrightarrow W^{(m_i)} .$$

In the monoalphabetic case, an arbitrary χ_s is selected from M and encryption is done with the sequence $X = [\chi_s , \chi_s , \chi_s , ...]$. It is in this case sufficient to take a singleton for M .

We start with the case $m_i = 1$ for all i .

Fig. 23. Cipher disk by Porta, 1563



F. L. Bauer, *Decrypted Secrets*

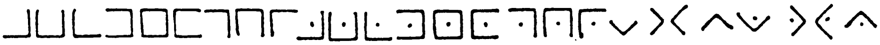
3.1 Case $V^{(1)} \dashrightarrow W$ (Unipartite Simple Substitution)

The case $V^{(1)} \dashrightarrow W$ deals with a unipartite simple substitution, for short just simple substitution (French *substitution simple ordinaire*).

3.1.1 $V \longrightarrow W$ **, heterogenous encryption without homophones and nulls.** This case is primeval. For W an alphabet of strangely formed, unusual graphemes is frequently used: Examples are known from Thailand, Persia, coptic Ethiopia and elsewhere. Such marks are used by Giovanni Battista Porta in his cipher disk (Fig. 23, see also Fig. 30). Charlemagne is said to have used such characters (Fig. 24).

The Freemasons' cipher is to be mentioned here. It goes back to the ancient 'pigpen' cipher, and in its modern form reads

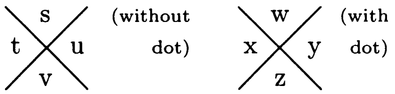
a b c d e f g h i j k l m n o p q r s t u v w x y z



It can be memorized by the schemes

a	b	c	(without dot)
d	e	f	
g	h	i	

j	k	l	(with dot)
m	n	o	
p	q	r	



As late as 1728, when it was broken by England's Deciphering Branch, the Czar Peter the Great used (besides nomenclators) a heterogenous substitution $V \longrightarrow W$ with a bizarre cipher alphabet.

Edgar Allan Poe, famous for his literary works, used a rather trivial alphabet of common printer's types in his story "The Gold-Bug" (Sect. 15.10.1).

In this class is also the bookseller's cipher for encrypting prices and dates, a one-to-one mapping $Z_{10} \longrightarrow Z_{26}$, generated by a password ('key-phrase' cipher). An example is

1	2	3	4	5	6	7	8	9	0
M	I	L	C	H	P	R	O	B	E ,

an encryption step with the password *milchprobe* ('milk sample') used in Germany over many years for specifying the packing date of butter.

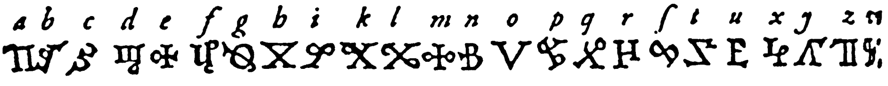


Fig. 24. Secret characters of Charlemagne

3.1.2 $V^{(1)} \dashrightarrow W$ **, heterogenous encryption with homophones and nulls.** Homophones are found already in Muslim sources, e.g., Qalqashandi 1412, and in a cipher used by the Duchy of Mantua in 1401 for an exchange of letters with Simeone de Crema. The vowels — typically the more frequent characters – were given homophones, a first sign of considerations to level the character frequency. Furthermore, W was enlarged by digits. The introduction of homophones practically enforces the introduction of nulls; otherwise homophones can be recognized easily by the constant pattern of letters surrounding them in frequent words.

3.2 Special Case $V \leftarrowtail\!\!\!\rightarrowtail V$ (Permutations)

In the case of a one-to-one mapping $V \leftarrowtail\!\!\!\rightarrowtail W$ among the examples in Sect. 3.1.1, W is called a mixed (cryptotext) alphabet of N characters (French *alphabet désordonné*, *alphabet incohérent*, German *umgeordnetes Geheimtextalphabet*), that matches a standard (plaintext) alphabet (French *alphabet ordonné*, German *Standard-Klartextalphabet*) V of N characters.

To define a substitution, it suffices to list in some way the matching pairs of plaintext characters and cryptotext characters, e.g., for $V \mathrel{\dot{\equiv}} W = Z_{26}$ (for the use of lower-case letters and small capitals see Sect. 2.5.6):

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

For encryption, it is more convenient, of course, to have the plaintext characters ordered into a standard (plaintext) alphabet; this gives a mixed (cryptotext) alphabet:

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

In mathematics, this 'substitution notation' is customary. For decryption, however, it is better to have the cryptotext characters ordered into a standard (cryptotext) alphabet; this gives a mixed (plaintext) alphabet:

b	l	w	n	d	h	g	u	v	o	r	z	i	e	s	j	p	a	m	k	t	q	c	y	f	x
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 new situation is given in the endomorphic case $V \mathrel{\dot{\equiv}} W$. Especially the one-to-one mapping $V \leftarrowtail\!\!\!\rightarrowtail V$ is then a permutation of V. The permutation $V \leftarrowtail\!\!\!\rightarrowtail V$ can be accomplished in electrical implementations by interchanging N wires (German *Umstecken*).

For permutations in particular, mathematics uses apart from the substitution notation the 'cycle notation'

(a r k t u h f y x h l b) (c w) (d e n) (g) (i m s o j p q v)

in which the distinction between lower-case letters and small capitals has to be abandoned. For encryption, one goes in the cycle where the plaintext character is found to the cyclically next character; for decryption, to the cyclically preceding character. Cycles of length 1 (1-cycles) are often suppressed – we shall not follow this habit.

3.2.1 The most ancient sources (apart from Egypt – we shall come back to this under 'code') show a self-reciprocal ('involutory') permutation of V: in

India, in the *Kāma-sūtra* of the writer *Vātsyāyana*, secret writing is mentioned as one of the sixty-four arts; *Mūladevīya* denotes the encrypting and decrypting procedure, which is a reflection ('involution'):

$$V \xleftrightarrow{2} V \ : \updownarrow \begin{array}{cccccccccc} \text{a} & \text{kh} & \text{gh} & \text{c} & \text{t} & \text{ñ} & \text{n} & \text{r} & \text{l} & \text{y} \\ \text{k} & \text{g} & \text{n} & \text{ṭ} & \text{p} & \text{ṇ} & \text{m} & \text{ṣ} & \text{s} & \text{ś} \end{array}$$

(the remaining characters are left invariant, so the permutation is not properly self-reciprocal). Plaintext and cryptotext alphabets of a self-reciprocal permutation are said to be reciprocal to each other.

In the Hebrew Holy Scripture boustrophedonic substitution, called *Athbash*, was used — although not for a cryptographic purpose — which would read in the Latin alphabet $V = Z_{20}$

$$V \xleftrightarrow{2} V \ : \updownarrow \begin{array}{cccccccccc} \text{a} & \text{b} & \text{c} & \text{d} & \text{e} & \text{f} & \text{g} & \text{h} & \text{i} & \text{l} \\ \text{z} & \text{v} & \text{t} & \text{s} & \text{r} & \text{q} & \text{p} & \text{o} & \text{n} & \text{m} \end{array}$$

. Such a substitution uses the reversed ('inverse') alphabet. In the case of the reflection

$$V \xleftrightarrow{2} V \ : \updownarrow \begin{array}{ccccccccccc} \text{a} & \text{b} & \text{c} & \text{d} & \text{e} & \text{f} & \text{g} & \text{h} & \text{i} & \text{l} & \text{m} \\ \text{a} & \text{z} & \text{v} & \text{t} & \text{s} & \text{r} & \text{q} & \text{p} & \text{o} & \text{n} & \text{m} \end{array}$$

Charles Eyraud speaks of a complementary alphabet (French *alphabet complémentaire*), see Sect. 5.6. This permutation, however, is not properly self-reciprocal: /a/ and /m/ are left invariant.

Obvious is also a reflection with a shifted alphabet like the Hebrew *Albam*, used in 1589 by the Argentis with $V = Z_{20}$

$$V \xleftrightarrow{2} V \ : \updownarrow \begin{array}{cccccccccc} \text{a} & \text{b} & \text{c} & \text{d} & \text{e} & \text{f} & \text{g} & \text{h} & \text{i} & \text{l} \\ \text{m} & \text{n} & \text{o} & \text{p} & \text{q} & \text{r} & \text{s} & \text{t} & \text{v} & \text{z} \end{array}$$

or the one used by Giovanni Battista Porta in 1563 (see Fig. 53) with $V = Z_{22}$

$$V \xleftrightarrow{2} V \ : \updownarrow \begin{array}{ccccccccccc} \text{a} & \text{b} & \text{c} & \text{d} & \text{e} & \text{f} & \text{g} & \text{h} & \text{i} & \text{l} & \text{m} \\ \text{n} & \text{o} & \text{p} & \text{q} & \text{r} & \text{s} & \text{t} & \text{v} & \text{x} & \text{y} & \text{z} \end{array} \ .$$

The most general boustrophedonic case, showing the use of a password, is presented by the following example: ($V = Z_{26}$)

$$V \xleftrightarrow{2} V \ : \updownarrow \begin{array}{ccccccccccccc} \text{a} & \text{n} & \text{g} & \text{e} & \text{r} & \text{s} & \text{b} & \text{c} & \text{d} & \text{f} & \text{h} & \text{i} & \text{j} \\ \text{z} & \text{y} & \text{x} & \text{w} & \text{v} & \text{u} & \text{t} & \text{q} & \text{p} & \text{o} & \text{m} & \text{l} & \text{k} \end{array} \ .$$

Reflections have, apart from the advantage of a compact notation, the property which some people have held to be of great importance that encryption and decryption steps coincide.

In the cycle notation of permutations, the last five examples would read (with cycle outsets ordered alphabetically):

(a,z) (b,v) (c,t) (d,s) (e,r) (f,q) (g,p) (h,o) (i,n) (l,m)
(a) (b,z) (c,v) (d,t) (e,s) (f,r) (g,q) (h,p) (i,o) (l,n) (m)
(a,m) (b,n) (c,o) (d,p) (e,q) (f,r) (g,s) (h,t) (i,v) (l,z)
(a,n) (b,o) (c,p) (d,q) (e,r) (f,s) (g,t) (h,v) (i,x) (l,y) (m,z)
(a,z) (b,t) (c,q) (d,p) (e,w) (f,o) (g,x) (h,m) (i,l) (j,k) (n,y) (r,v) (s,u)

Properly self-reciprocal is a permutation without 1-cycles, which means solely with 2-cycles ('swaps'). It is the target of cryptanalytic attacks (Sect. 14.1) that cease to work if some of the cycles are 1-cycles ('females').

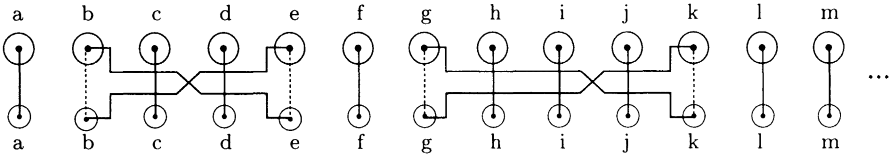


Fig. 25. Self-reciprocal permutation by cross-plugging with double-ended connectors

For a binary alphabet $V = Z_2$, the sole nontrivial permutation is a reflection: $V \overset{2}{\longleftrightarrow} V : \updownarrow \begin{smallmatrix} O \\ L \end{smallmatrix}$.

3.2.2 In electrical implementations, reflections are accomplished by swapping pairs of wires, simply by using double-ended connectors (Fig. 25). Such reflections were used in the ENIGMA plugboard (German *Steckerbrett*).

The number $d(k, N)$ of reflections depends on N and the number k of cinch plugs used:

$$d(k,N) = \frac{N!}{2^k \cdot (N-2k)! \cdot k!} = \binom{N}{2k} \cdot \frac{(2k)!}{2^k k!} = \binom{N}{2k} \cdot (2k-1)!! \text{ , where}$$

$$(2k-1)!! = (2k-1) \cdot (2k-3) \cdot \ \dots \ \cdot 5 \cdot 3 \cdot 1 = \frac{(2k)!}{2^k k!} \ .$$

Properly self-reciprocal permutations ('genuine' reflections) require $N = 2\nu$ to be even. The number $d(\frac{N}{2}, N)$ of all genuine reflections is then (with a relative error $< 10^{-3}$ for $N \geq 6$)

$$d(\frac{N}{2}, N) = (N-1)!! = (N-1) \cdot (N-3) \cdot \ \dots \ \cdot 5 \cdot 3 \cdot 1 \approx \frac{\sqrt{N!}}{\sqrt[4]{\pi \cdot (2N+1)/4)}} \ .$$

A good upper limit for $(N-1)!!$ is $(N!)^{\frac{1}{2}}$.

For fixed N , however, $d(k, N)$ is maximal for some $k < \nu$:

$d(5,26) \approx 5.02 \cdot 10^9$, $d(6,26) \approx 1.00 \cdot 10^{11}$, $d(7,26) \approx 1.31 \cdot 10^{12}$,
$d(8,26) \approx 1.08 \cdot 10^{13}$, $d(9,26) \approx 5.38 \cdot 10^{13}$, $d(10,26) \approx 1.51 \cdot 10^{14}$,
$d(11,26) \approx 2.06 \cdot 10^{14}$, $d(12,26) \approx 1.03 \cdot 10^{14}$, $d(13,26) \approx 7.91 \cdot 10^{12}$,

and $d(3,10) = 3150$, $d(4,10) = 4725$, $d(5,10) = 945$.

The ENIGMA I of the *Reichswehr* of 1930 originally used six double-ended two-line connectors, the *Wehrmacht* ENIGMA, beginning October 1, 1936, five to eight, from January 1, 1939 seven to ten, and from August 19, 1939 ten double-ended two-line connectors for cross-plugging.

3.2.3 A compact notation describes also the monocyclic permutation, the order of which is N:

e.g., with $N = 20$ the cycle of the standard alphabet Z_{20}

$V \overset{N}{\longleftrightarrow} V$: (a b c d e f g h i l m n o p q r s t v x)

or its third power

$V \overset{N}{\longleftrightarrow} V$: (a d g l o r v b e h m p s x c f i n q t) ;

in substitution notation

a b c d e f g h i l m n o p q r s t v x
B C D E F G H I L M N O P Q R S T V X A ,

a b c d e f g h i l m n o p q r s t v x
D E F G H I L M N O P Q R S T V X A B C .

The last encryption step was used by Julius Caesar (according to Suetonius), counting upwards three letters in the alphabet. His successor Augustus, inferior in several respects to Caesar, used the first encryption step (possibly he could not safely count up to three); Suetonius said he also replaced x by AA.

Every power of the cycle of the standard alphabet yields a CAESAR alphabet. We shall come back to this in Chapter 5 (CAESAR addition). But note: while the two encryption steps above are of the order twenty, the second power has only the order ten, and the tenth power has only the order two: it is a reflection as studied above. The $(N-1)$-th power is the inverse of the first power and yields the decryption step.

A monoalphabetic substitution with a CAESAR encryption step was introduced in 1915 in the Russian army after it turned out to be impossible to expect the staffs to use anything more complicated. For the Prussian Ludwig Deubner and the Austrian Hermann Pokorny, heads of the cryptanalytic services of their respective countries, it was a pleasantly simple matter to decrypt these messages.

By its very nature, a track on a disk, the rim of a washer, or a strip closed to form a ring can be used to represent a full cycle. Such gadgets have found wide use and were employed in a particular way (Sect. 7.5.3) by Thomas Jefferson (around 1795) and Étienne Bazeries (1891). The q-th power of the monocyclic permutation is obtained by counting within the cycle in steps of q characters.

3.2.4 For non-selfreciprocal and non-cyclic $V \longleftrightarrow V$, in the most general case of a mixed alphabet (French *alphabet désordonné*, German *permutiertes Alphabet*), substitution notation is normally used:

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

The short cycle notation is useful here, too. It shows the decomposition

$V \longleftrightarrow V$: (a s n h y x w v q l f i) (b e r m g t o j) (c) (d u p k) (z) ,

into one 12-cycle, one 8-cycle, one 4-cycle, and two 1-cycles (cycle partition 12+8+4+1+1).

(1) More mixed alphabets are obtained by a cyclic shift of one of the two lines in the substitution notation (shifted mixed alphabets, French *alphabet désordonné parallèle*, German *verschobenes permutiertes Alphabet*):

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

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

in cycle notation

(a e i b c u q m h) (d r n j) (f t p l g y z s o k) (v) (w) (x) ,

(a c r o l h b u v w x z e t q n k g) (f y s p m j) (d i) .

(2) Iterated substitution, also called 'raising to a higher power' produces the powers of a mixed alphabet, e.g., from the substitution SECURITY... above, the second power gives

(a n y w q f) (b r g o) (c) (d p) (e m t j) (h x v l i s) (k u) (z) ,

with all cycles of even length being split in halves; in substitution notation

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

Shifting on the one hand, raising to a power on the other do not give the same thing in general; they are two utterly different methods for producing a family of up to N (sometimes less) accompanying alphabets (Chapter 7).

3.2.5 The examples above show already the construction of an (endomorphic) simple substitution $V \longleftrightarrow V$ with the help of a password (French *mot-clef*, German *Kennwort, Losung*), possibly a mnemonic key or a key phrase. A classical method uses a word from V , writes its characters without repetitions and fills in alphabetic order with the characters not used. The method goes back to Giovanni Battista Argenti, around 1580. It was still a cryptologic standard even in the 20th century.[1]

This construction, however, is vulnerable: it may be easy to guess a missing part of the password (after all, the most frequent vowels /e/ and /a/ always are substituted by a letter from the password, if this has length 5 or more). A small consolation is that the password should not need much fill.

More cunning methods use therefore a reordering of the password, for example by writing it first in lines and reading it in columns (method of Charles Wheatstone, 1854, a transposition to be treated methodically in Sect. 6.2):

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

a	e	i	l	o	r	u	x
b	f	j	m	p	s	v	y
c	g	k	n	q	t	w	z
d	h						

This yields the alphabet

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

or in cycle notation

(a s h z w v j d x y k n o r i c l u t q p g m f b) (e)

with the 1-cycle (e) .

[1] Allowing repetitions is bad: it leads to polyphones, e.g., the 'key-phrase' cipher

a	b	c	d	e	f	g	h	i	j	l	m	n	o	p	q	r	s	t	u	v	x	y	z
L	E	G	O	U	V	E	R	N	E	M	E	N	T	P	R	O	V	I	S	O	I	R	E

and shortens the cryptotext character set (in our case to 14 characters).

A further method fills also the columns of the plaintext side in the alphabetic order of the letters of the password, in the example in the order

third, second, sixth, fifth, first, seventh, fourth, eighth column

with the result

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

n	d	a	u	k	h	r	x
o	e	b	v	l	i	s	y
p	f	c	w	m	j	t	z
q	g						

This results in the alphabet

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

or in cycle notation

(a c n s j q x y k r t v f m p l g z w o) (b d e) (h i) (u) .

The method can also be used for the construction of cycles. The sentence *évitez les courants d'air*, "avoid drafts" (Bazeries, Sect. 7.4.3) produces the cycle

$V \overset{N}{\longleftrightarrow} V$: (e v i t z l s c o u r a n d b f g h j k m p q x y)

3.2.6 The following table gives for $N = 26$, for $N = 10$ and for $N = 2$ a survey of the number $Z(N)$ of available alphabets $V \longleftrightarrow V$:

number of permutations	$Z(N)$	$Z(26)$	$Z(10)$	$Z(2)$
total	$N\,!$	$4.03 \cdot 10^{26}$	3 628 800	2
monocyclic	$(N-1)\,!$	$1.55 \cdot 10^{25}$	362 880	1
reflections total	$\approx N \cdot (N\,!)^{\frac{1}{2}}$	$5.33 \cdot 10^{14}$	9 496	2
genuine reflections	$\approx (N\,!)^{\frac{1}{2}}$	$7.91 \cdot 10^{12}$	945	1
derived from meaningful passwords (mnemonic words)		$10^4 \ldots 10^6$		

3.2.7 To mechanize a substitution, the fixed matching of the plaintext and the cryptotext characters, as found in the substitution notation, can be arranged on a cylinder or on a strip. Two windows allow one to see just two matching characters at any given moment. The windows can be arranged so that only the master sees the plaintext character, while the clerk only sees the cryptotext window and cannot grasp the meaning of the message (Sect. 7.5.2, Gripenstierna's machine, Fig. 54).

A selection from the N accompanying shifted alphabets is obtained if one of the windows can be moved. Another possibility is to shift the plaintext alphabet with respect to the cryptotext alphabet. This leads to the use of two disks (Fig. 26) or two strips (Fig. 27). In the latter case it is necessary to repeat one of the alphabets (duplication).

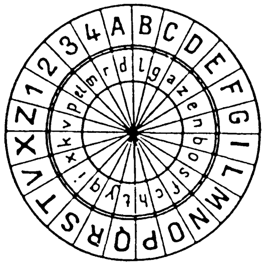


Fig. 26.
Cipher disk of Leon Battista Alberti (Lange-Soudart 1935)

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	b	c	d	e	f	g	h	i	j	k	l	m	...
						S	E	C	U	R	I	T	Y	A	B	D	F	G	H	J	K	L	M	N	O	P	Q	V	W	X	Z								

Fig. 27. Cipher slide with duplicated plaintext alphabet

Cipher disks (French *cadran*, German *Chiffrierscheibe*), mechanical tools for general substitution with shifted mixed alphabets, were described as early as 1466 by Leon Battista Alberti[2] (see Plate B). Cipher slides (French *reglette*, German *Chiffrierschieber*) were used in Elizabethan England around 1600. In the 19th century they were named *Saint-Cyr* slides after the famous French Military Academy. Cipher rods (French *bâtons*, German *Chiffrierstäbchen*) serve the same purpose.

3.2.8 Mechanizing a monocyclic permutation can also start from the cycle notation. The cycle of characters is again arranged on a cylinder or on a strip (in the latter case the first character must be duplicated). Two neighboring windows allow just two characters to be seen at any given moment, the left one of which is the plaintext character, the other one the corresponding cryptotext character.

A selection from the (up to N) accompanying powers of a mixed alphabet is obtained if the distance between the windows can be changed. In the case of a strip, it is then necessary to duplicate the whole cycle. The q-th power of the monocyclic permutation is obtained if the windows have a distance of q characters. This can also be achieved with a slide (Fig. 28 for $q = 14$).

												↓						14								↑													
S	E	C	U	R	I	T	Y	A	B	D	F	G	H	J	K	L	M	N	O	P	Q	V	W	X	Z	S	E	C	U	R	I	T	Y	A	B	D	F	G	...

Fig. 28. Cipher slide for powers of an alphabet

[2] In Alberti's illustration, differing from modern usage, capital letters are used for plaintext, small letters for cryptotext. The character /et/ presumably stands for the symbol & . The initial setting of the disk is established by lining up a key letter, say D , with a fixed character, say /a/.

3.3 Case $V^{(1)} \dashrightarrow W^m$ (Multipartite Simple Substitution)

3.3.1 $m = 2$, **bipartite simple substitution** $V^{(1)} \dashrightarrow W^2$. Substitution by bigrams (bipartite substitution) was known in antiquity, and Polybios described a quinary ($|W| = 5$) bipartite substitution for Greek letters. In a modern form, Z_{25} is inscribed into a 5×5 checkerboard:

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

or

	1	2	3	4	5
1	a	f	l	q	v
2	b	g	m	r	w
3	c	h	n	s	x
4	d	i	o	t	y
5	e	k	p	u	z

Decryption with the 'Polybios square' on the right hand side gives for the text semagram

33515141234333514512432411343411343442331144424333

of Sect. 1.2, Fig. 3, the plaintext

needmoneyforassassination .

While Polybios described how torches can represent the numbers 1 – 5, knock signals are used for it in more modern times. The special $Z_{25} \longrightarrow Z_5 \times Z_5$ cipher above is the ubiquitous, truly international knock cipher, used in jails from Alcatraz to Ploetzensee by criminals as much as by political prisoners. The normal speed of transmission is 8–15 words per minute.

In Czarist Russia, such a knock-cipher (with the Russian alphabet in a 6×6 square) was common and came to Western Europe with Russian anarchists as part of the 'Nihilist cipher' (Sect. 9.4.4), it was also used steganographically, see Sect. 1.2. Alexander Solzhenitsyn, in *The Gulag Archipeligo*, reported on its more recent use in the Soviet Union.

In general, a password is used, which is inscribed line by line and the remaining characters filled in. The count Honoré de Mirabeau, a French revolutionary in the 18th century, used this method in his correspondence with the Marquise Sophie de Monnier — he, too, used it steganographically and added 6 7 8 9 0 as nulls.

The ADFGVX system, invented by Fritz Nebel (1891–1967), which was installed in 1918 on the German Western Front under Quartermaster General Erich Ludendorff for wireless transmission (for the cryptotext alphabet Z_6 see Sect. 2.5.2), worked with $|W| = 6$ and checkerboards like

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	l	0	j	d
G	5	s	i	y	h	u
V	p	1	v	b	6	r
X	e	q	7	t	2	g

Rectangular arrays are used, too. Giovanni Battista Argenti, around 1580, used the following scheme (with $W = Z_{10}$)

	0	1	2	3	4	5	6	7	8	9
1	p	i	e	t	r	o	a	b	c	d
2	f	g	h	l	m	n	q	s	u	z

with the very first application of a password.

In general, the bipartite substitution leaves ample space for homophones:

	1	2	3	4	5	6	7	8	9
9, 6, 3	a	b	c	d	e	f	g	h	i
8, 5, 2	j	k	l	m	n	o	p	q	r
7, 4, 1	s	t	u	v	w	x	y	z	.

In this example the character 0 may serve as a null. 0, originally *nulla ziffra*, still is not taken seriously everywhere.

Preferably, homophones should smooth out the character frequencies in the cryptotext. Since the letters e t a o n i r s h in English have altogether a frequency around 70 % a good balance is reached by

	1	2	3	4	5	6	7	8	9	
4,5,6,7,8,9,0	e	t	a	o	n	i	r	s	h	71.09 %
2,3	b	c	d	f	g	j	k	l	m	19.46 %
1	p	q	u	v	w	x	y	z		9.45 % .

Another method uses a 4-letter password and decides in this way on the outset of the cycles (**00**...24), (**25**...49), (**50**...74), (**75**...99) in defining (with $V = Z_{25}$ and $W = Z_{10}^2$) a homophonic cipher, e.g., with the password *KILO*:

	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
K	16	17	18	19	20	21	22	23	24	**00**	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
I	42	43	44	45	46	47	48	49	**25**	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
L	65	66	67	68	69	70	71	72	73	74	**50**	51	52	53	54	55	56	57	58	59	60	61	62	63	64
O	87	88	89	90	91	92	93	94	95	96	97	98	99	**75**	76	77	78	79	80	81	82	83	84	85	86

A denary ($|W| = 10$) bipartite cipher does not have to have homophones — the substitution does not have to be surjective and some pairs can be left unused. Such a cipher was used by the Swedish baronet Fridric Gripenstierna — possibly based on a proposal of Christopher Polheim. A funny form of a bipartite cipher with homophones was agreed upon during the development of the atom bomb by Brig. Gen. Leslie R. Groves and Lt. Col. Peer da Silva in Los Alamos (Fig. 29), to be used in telephone conversations for veiling special names and places. The point is that it takes time to look up the letters, and thus homophones are selected more at random than normally, when the encipherer is biased.

3.3.2 $m = 3$, tripartite simple substitution $V^{(1)} \dashrightarrow W^3$. Substitution by trigrams (tripartite substitution) was proposed by Trithemius in the *Polygraphiæ*, with $|W| = 3$ (note that $3^3 = 27 > 26$) for steganographic reasons. Otherwise, ternary substitutions like this one are rare.

1	2	3	4	5	6	7	8	9	0	
I	P	I		O	U	O		P	N	1
W	E	U	T	E	K		L	O		2
E	U	G	N	B	T	N		S	T	3
T	A	Z	M	D		I	O	E		4
S	V	T	J		E		Y		H	5
N	A	O	L	N	S	U	G	O	E	6
	C	B	A	F	R	S		I	R	7
I	C	W	Y	R	U	A	M		N	8
M	V	T		H	P	D	I	X	Q	9
L	S	R	E	T	D	E	A	H	E	0

Fig. 29. Bipartite cipher, used in Los Alamos in 1944 for telephone conversations

3.3.3 $m = 5$, quinpartite simple substitution $V^{(1)} \dashrightarrow W^5$. Substitution by groups of five cryptotext characters (quinpartite substitution) with $|W| = 2$ was used by Francis Bacon in connection with steganographic means (note that $2^5 = 32 > 26$). Quinpartite binary encryption was resurrected in the cipher machine of Vernam in 1918 (Sect. 8.3.2) and in the Second World War crypto-teletype machines Siemens T52 (*Geheimschreiber*) and Lorenz SZ40/42 (*Schlüsselzusatz*), see Sect. 9.1.3.

3.3.4 $m = 8$, octopartite simple substitution $V^{(1)} \dashrightarrow W^8$. Again with $|W| = 2$ (8-bit code, binary EBCDIC code, ASCII code with checkbit), this octopartite simple substitution coincides with monopartite substitution by bytes ($\mathbb{Z}_{256}$) in modern computers.

3.4 The General Case $V^{(1)} \dashrightarrow W^{(m)}$, Straddling

The general case $V^{(1)} \dashrightarrow W^{(m)}$ plainly invites the use of null and homophones.

Simeone di Crema in Mantua (1401) used just homophones (with $m = 1$). With $m = 2$, apart from the use of homophones and nulls an important new thought comes into play: straddling (German *Spreizen*) of the alphabet, the mapping of V into $W^1 \cup W^2$. A cipher used at the Holy See, the papal court, devised by Matteo Argenti after 1590, shows homophones, nulls, and straddling. For an alphabet $\mathbb{Z}_{24}$ enriched by /et/, /con/, /non/, /che/ and with 5, 7 serving as nulls, the encryption step $\mathbb{Z}_{24}^{(1)} \dashrightarrow \mathbb{Z}_{10}^1 \cup \mathbb{Z}_{10}^2$ is

a	b	c	d	e	f	g	h	i	l	m	n	o
1	86	02	20	62 82	22	06	60	3	24	26	84	9

p	q	r	s	t	v	z	et	con	non	che	ε
66	68	28	42	80 40	04	88	08	64	00	44	5 7

3.4.1 Encryption steps with straddling are subject to the restriction that the encryption induced by them should turn out to be left-unique – this means that the hiatuses between the one-letter and the two-letter cipher elements and thus the correct decomposition are well determined. As stated in Sect. 2.4, G. B. and M. Argenti were aware of this. Their ciphers fulfill the following conditions: W is divided up into characters used for one-character cipher elements, $W' = \{1, 3, 5, 7, 9\}$ and characters used for two-character cipher elements to begin with, $W'' = \{0, 2, 4, 6, 8\}$. The Argentis made the mistake of restricting also the second character of these to W''. This exposes the straddling. Otherwise, they made some more practical recommendations: to suppress the u following the q and to suppress a duplicated letter.

The so-called spy ciphers used by the Soviet NKVD and its followers are straddling ciphers. They have been disclosed by convicted spies. By analogy with Polybios squares they are described by rectangular arrays too, e.g.,

	0	1	2	3	4	5	6	7	8	9
	s	i	o	e	r	a	t	n		
8	c	x	u	d	j	p	z	b	k	q
9	.	w	f	l	/	g	m	y	h	v

(*)

where the first line contains the one-letter cipher elements.

With $W = Z_{10}$ 28 cipher elements are obtainable, enough for Z_{26} and two special characters, . for 'stop' and / for letter-figure swap. Because this cipher was subjected to further encryption ('closing', Sect. 9.2.1), it was tolerable to encrypt figures – after sending a letter-figure swap sign – by identical figure twins, a safeguard against transmission errors.

For the construction of this array passwords have been used, too. Dr. Per Meurling, a Swedish fellow traveler, did it 1937 as follows: He wrote down an 8-letter password (M. Delvayo was a Spanish communist) and below it the remaining alphabet; the columns were numbered backwards:

	0	9	8	7	6	5	4	3	2	1
	m	d	e	l	v	a	y	o		
1	b	c	f	g	h	i	j	k	n	p
2	q	r	s	t	u	w	x	z	.	/

This procedure had the disadvantage that not at all the most frequent letters obtained 1-figure ciphers. This disadvantage was also shared by the method the Swedish spy Bertil Eriksson used in 1941: He numbered the columns according to the alphabetic order of the letters occurring in the password (Sect. 3.2.5):

	6	0	8	7	5	4	9	1	2	3
3	p	a	u	s	o	m	v	e	j	k
9	b	c	d	f	g	h	i	l	n	q
	r	t	w	x	y	z				

The password was taken from a Swedish translation of Jaroslav Hašek's novel *Paus, som Svejk själv avbröt ....* Since encryption of the most frequent letters by 1-figure ciphers also shortens the telegraphic transmission time, the NKVD arrived in 1940 at a construction method that took this into account.

Max Clausen, wireless operator of the Russian spy Dr. Richard Sorge in Tokyo, had to memorize the sentence *"a sin to err"* (very good advice for a spy), containing the eight most frequent letters in English, 65.2 % altogether. Beginning with a password /subway/, a rectangle was started and filled with the remaining letters. Thereupon, columnwise from left to right in the order of their appearance, first, the letters from the set {a s i n t o e r} were assigned the numbers 0 ... 7; second, the remaining letters were assigned the numbers 80 ... 99 :

s	u	b	w	a	y
0	82	87	91	5	97
c	d	e	f	g	h
80	83	3	92	95	98
i	j	k	l	m	n
1	84	88	93	96	7
o	p	q	r	t	v
2	85	89	4	6	99
x	z	.	/		
81	86	90	94		

In this way, the Polybios rectangle marked above by (*) is obtained in more compact notation.

For the cyrillic alphabet, a subdivision into seven 1-figure ciphers and thirty 2-figure ciphers, altogether 37 ciphers, is suitable; it allows 5 special characters. A method that was given away by the deserted agent Reino Hayhanen, an aide to the high-ranking Russian spy Rudolf Abel, used a Russian word like СНЕГОПАД ('snowfall'), the first seven letters of which have a total frequency of 44.3 %. The rectangle was formed as usual

С	Н	Е	Г	О	П	А	.	.	.
Б	В	Д	Ж	З	И	Й	К	Л	М
Р	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ы	Ь	Э	Ю	Я	.	.	.	.	.

and then rearranged with the help of a key that was changed from message to message and was to be found at a prearranged place within the cipher message. Finally, a closing encryption (Sect. 9.2.1) was made.

3.4.2 On this occasion, it was also disclosed that the Russians used what became to be called "Russian copulation": the message was cut into two parts of roughly the same length and these parts were joined with the first after the second, burying in this way the conspicuous standard phrases at beginning and end somewhere in the middle.

Winston Churchill called Russia "a riddle wrapped in a mystery inside an enigma." This is also true for Russian cryptology.