

# Playfair and ADFGVX / ADFGVX

19. (a) Use the Playfair cipher with key *diskjockey* to encrypt each of the strings of plaintext
- the shipment will arrive at noon
  - lay low until friday
  - always use the back door
  - the phone is bugged
- (b) Decrypt each of the following ciphertexts that came from the Playfair cipher of part (a):
- RBIABDIGTPSZ
  - QMBGDTYASKCZXKPKCIDUICTPYBQM
  - REBSLUMNGYXYNBLFCR
  - QTBPCPCDZLXYBQTDMYIKDTKUFGEQD  
SIYEITBQGYGDGAKW

TABLE 1.4 ADFGVX Table

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

23. (a) Use the ADFGVX cipher with key *PARIS* to encrypt each of the strings of plaintext
- the shipment will arrive at noon
  - lay low until friday
  - always use the back door
  - the phone is bugged
- (b) Decrypt each of the following ciphertexts that came from the ADFGVX cipher of part (a):
- VVVDXDVDDXVDDD
  - XXDDGADAXVVXGGXVXXGVXGXGVGGD  
DXDAGDGGDADAXAGAVAFVXVGVDXGDXA
  - DVDGVGDGDFDDVDFVXVGVGDVDGD  
VGDVDDGDVD
  - XFDDDDAXDDGXXDVVVFDDADXXDGD  
VADVVDXAVAXXDGFDXDAGAFDGD  
DDVVGDFDG
25. Do identical adjacent pairs of plaintext typically encode to the same four-letter ciphertext strings under the ADFGVX cipher? Explain your answer.
26. Are there any problems with procedure and/or loss of security with the ADFGVX cipher if one were to use a keyword with duplicated letters (such as *LONDON*)? Explain your answer.