Polybius 密码

Polybius 密码也称棋盘密码，是利用波利比奥斯方阵（Polybius Square）进行加密的密码方式。

假设我们需要发送明文消息“Attack at once”， 用一套秘密混杂的字母表填满波利比奥斯方阵，像是这样：

	A	**D**	**F**	**G**	**X**
A	b	t	a	l	p
D	d	h	o	z	k
F	q	f	v	s	n
G	g	j	c	u	x
X	m	r	e	w	y

i 和 j 视为同一个字母，使字母数量符合 5 × 5 格。之所以选择这五个字母，是因为它们译成摩斯密码时不容易混淆，可以降低传输错误的机率。使用这个方格，找出明文字母在这个方格的位置，再以那个字母所在的行名称和列名称代替这个字母。

可将该消息转换成处理过的分解形式。

明文：A T T A C K A T O N C E

密文：AF AD AD AF GF DX AF AD DF FX GF XF

A、D、F、G、X 也可以用数字 1、2、3、4、5 来代替，这样密文就成了：

13 12 12 13 43 25 13 12 23 35 43 53

ADFGX/ADFGVX 密码

1.ADFGX 密码

1918 年，第一次世界大战将要结束时，法军截获了一份德军电报，电文中的所有单词都由 A、D、F、G、X 五个字母拼成，因此被称为 ADFGX 密码。

ADFGX 密码是 1918 年 3 月由德军上校 Fritz Nebel 发明的，是结合了 Polybius 密码和置换密码的双重加密方案。A、D、F、G、X 即 Polybius 方阵中的前 5 个字母。

明文：A T T A C K A T O N C E

经过 Polybius 变换：AF AD AD AF GF DX AF AD DF FX GF XF

下一步，利用一个移位密钥加密。假设密钥是“CARGO”，将之写在新格子的第一行。再将上一阶段的密文按行写进新方格里。

C A R G O

A F A D A

D A F G F

D X A F A

D D F F X

G F X F X

最后，密钥按照字母表顺序“ACGOR”排序，再按照此顺序依次读出每个字母下面的整列，形成新密文。如下：

FAXDF ADDDG DGFFF AFAXX AFAFX

在实际应用中，移位密钥通常有两打字符那么长，且分解密钥和移位密钥都是每天更换的。

2.ADFGVX 密码：

在 1918 年 6 月，再加入一个字 V 扩充。变成以 6×6 格共 36 个字符加密。这使得所有英文字母（不再将 I 和 J 视为同一个字）以及数字 0 到 9 都可混合使用，这次增改是因为以原来的加密法发送含有大量数字的消息有问题。