ADFGVX – Part 1
"Painvin's Analysis"

Author: Volker Simon

July 2011

Introduction

An encrypted message has been intercepted from an adversary messenger at the late evening. Georges Painvin, a French army officer, recognizes the ciphertext as a message which has been encrypted with the ADFGVX cipher.

The ciphertext reads as follows:
ADGG AADG FDFA AVFD DAAV GDFF DXFG
AFAA DDDF GFGD FFAG VDDF AFFG AADG
AAAG AAGD FFDA GFAA GGAG DGAA AAAD
GGAD DAAA GAFA GGGA ADAD FAAA

©David Kahn Collection

Georges Painvin knows that his troops are in danger. There is not much time for him to decrypt the ciphertext using pen, paper and his mind.

The ciphertext contains only upper-case characters and the frequency of the three most-frequent characters (E, N, I) within the plaintext is the same as they occur usually in the German language. That means "E" has the highest occurence rate, "N" second highest and "I" the third highest. Neither the substitution key nor the transposition key is known to Georges Painvin. But he knows that the adversary has simply used a German 4 character word as a substitution key and 4 digits for the transposition key.

Are you able to help Georges Painvin by decrypting the ciphertext? Please send us the plaintext.