Universidade de São Paulo
Instituto de Ciências Matemáticas e de Computação

SSC0547 -Engenharia de Segurança
Professora Kalinka Regina Castelo Branco

CRIPTOGRAFIA CLÁSSICA

Implementação do Algoritmo ADFGVX

Trabalho de Curso Desenvolvido pelos Alunos

Ubiratan Soares (5634292)
Ulisses Soares (5377365)
Leonardo Barbosa Alves (5889522)

São Carlos, 07 de Dezembro de 2010

História da Cifra ADFGVX

A cifra ADFGVX foi utilizada por soldados alemães durante a Primeira Guerra Mundial para cifrar mensagens no campo de batalha. Inventada pelo coronel alemão Fritz Nebel e colocada em prática em 1918, essa cifra combina técnicas de substituição e transposição de colunas, sendo uma evolução da cifra ADFGX [1].

A razão para o nome ADFGVX está no fato das comunicações da época se darem pelo famoso código Morse. A letras que formam o nome da cifra são bastante distintas nesse código, de forma que o processo de cifragem - que leva a um texto que contém somente as letras A, D, F, G, V e X - minimizava os erros de transmissão por parte dos operadores de telégrafos.

A ADFGVX foi criptoanalisada com sucesso pelo militar frânces Georges Painvin, em um esforço físico e mental que o levou a ficar doente e perder vários quilos durante o processo[2].

O Algoritmo ADFGVX

A chave da ADFGVX é composta por dois itens. O primeiro deles é uma tabela 6 x 6 indexada por linhas e colunas com as letras que compõem o nome da cifra, como abaixo. Nessa tabela, emissor e receptor possuem um mapeamento das 26 letras do alfabeto e dos 10 dígitos,

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

que deve ser comum entre emissor e receptor.

O primeiro passo do processo de cifragem está associado à substituição, e consistem em mapear as letras de mensagem cifrada nós rótulos de linha e coluna da tabela ADFGVX. Assim, cada letra do texto plano será mapeada em dois caracters no texto cifrado, como pode ser visto

H	E	L	L	O		M	Y		D	E	A	R
VG	AF	GD	GD	GG		AV	FD		AA	AG	AG	XV

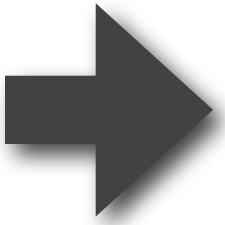
para o exemplo a seguir:

Se o processo de cifragem consistisse somente desse passo, a cifra seria vulnerável à ataques por análise de frequência[2]. Para contornar esse tipo técnica, é então realizada a transposição com a segunda parte da chave, que deve ser uma palavra comum para emissor e receptor.

O processo de transposição se dá como a seguir. Suponha que a palavra chave do dia seja "JOHN", com 4 letras. São então geradas 4 colunas para transposição rotuladas por J, O, N e H, e o texto cifrado é colocado linha a linha, da esquerda para a direita e de cima para baixo ao longo dessas colunas. A seguir, essas colunas são rearranjadas, de maneira que os rótulos fiquem em

H	E
L	L
O	M
Y	D
E	A
R	

J	O	N	H
V	G	A	F
G	D	G	D
G	G	A	V
F	D	A	A
A	G	A	G
X	V		



H	J	N	O
A	V	F	G
G	G	D	D
A	G	V	G
A	F	A	D
A	A	G	G
	X		V

ordem alfabética.

O texto cifrado é então obtido lendo-se cada coluna de cima para baixo, da esquerda para direita.

TEXTO CIFRADO = **A G A A A V G G F A X F D V A G G D G D G V**

H	J	N	O
A	V	F	G
G	G	D	D
A	G	V	G
A	F	A	D
A	A	G	G
	X		V

(1) AGAAA

(2) VGGFAX

(3) FDVAG

(4) GDGDGV

Um detalhe importante a respeito da segunda etapa de cifragem é que a palavra-chave escolhida não pode possuir caracteres repetidos. Isso evita ambiguidades no processo de decifragem.

Compilando e Executando

A implementação do ADFGVX foi realizada em linguagem Java, por essa ser interoperável e possuir uma rica API com ferramentas úteis.

Para compilar o programa, é necessário ter o ambiente Java instalado. Mais detalhes podem ser obtidos a partir de http://www.java.com .

Com esse requisito atendido, compila-se o programa via linha de comando com

```
$-> javac Adfgvx.java
```

Para executar,

```
$-> java Adfgvx
```

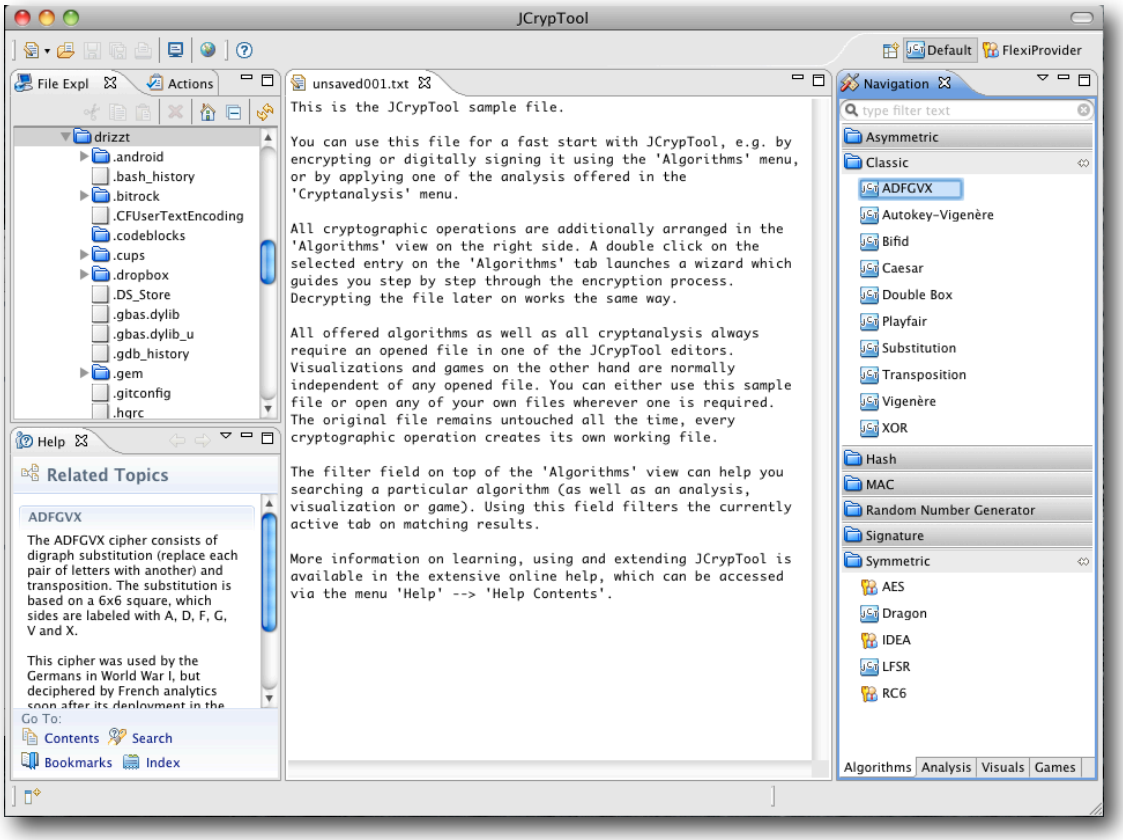
O programa é executado em ambiente terminal. A matriz inicial ADFGVX é gerada aleatoriamente, e exibida para o usuário logo após esse fornecer a chave para transposição. O programa então executa a cifragem e decifragem de acordo com o algoritmo descrito, conforme pode ser conferido nos métodos da **classe Adfgvx** no código-fonte.

Criptoanálise com a Ferramenta JCripTool

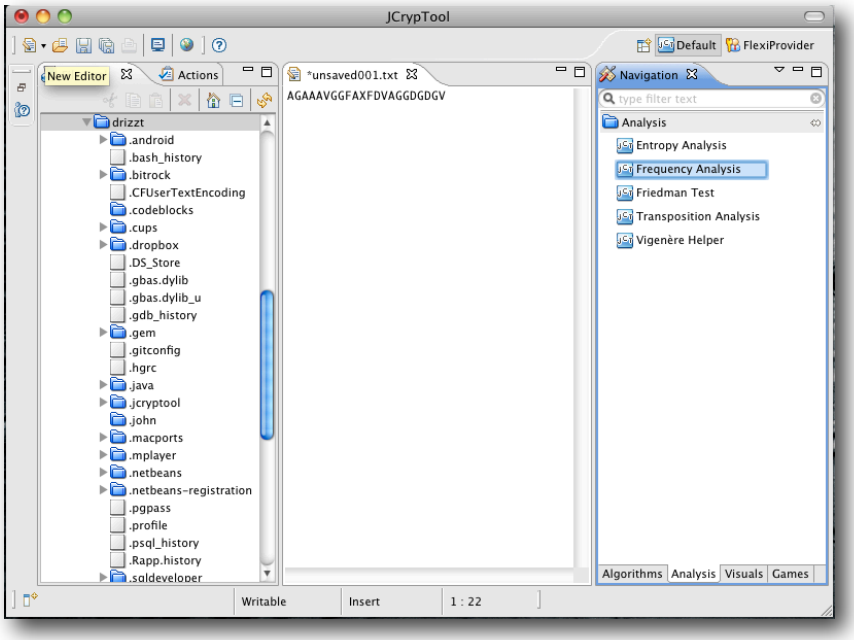
A ferramenta JCripTool [4] tem a proposta de ser uma opção para e-learning de métodos clássicos de criptografia. Escrita em Java e de código aberto, o JCripTool oferece diversos modos de análise para textos cifrados, com guias de evolução que ajudam o criptoanalista a ter uma melhor orientação para palpites e desfazer equívocos na batalha contra as cifras de maneira mais fácil e intuitiva.

No sentido de explorar as potencialidades do JCripTool para a cifra ADFGVX (que possui um módulo de implementação nativo) foi utilizado o recurso de análise de frequência para evidenciar que a cifra implementada é realmente invulnerável a esse ataque.

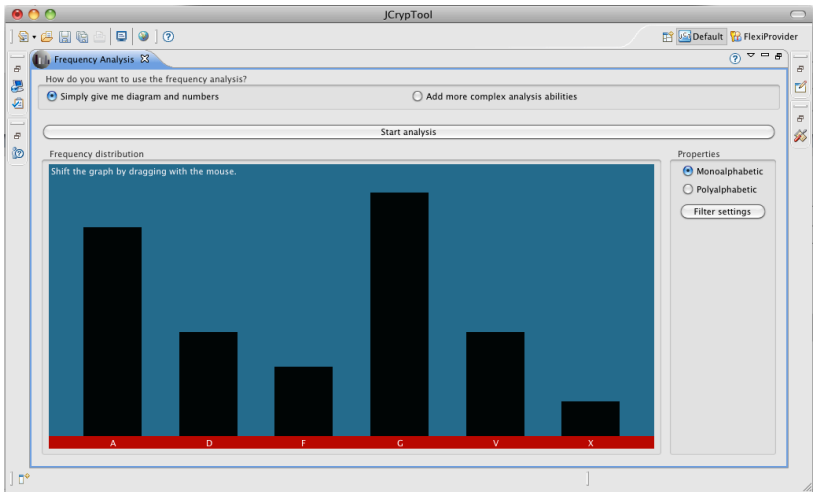
A tela inicial do JCripTool é como a seguir. Nela podemos observar um espaço central de trabalho, no qual o texto corrente pode ser substituído pelo texto a ser cifrado ou decifrado. Um

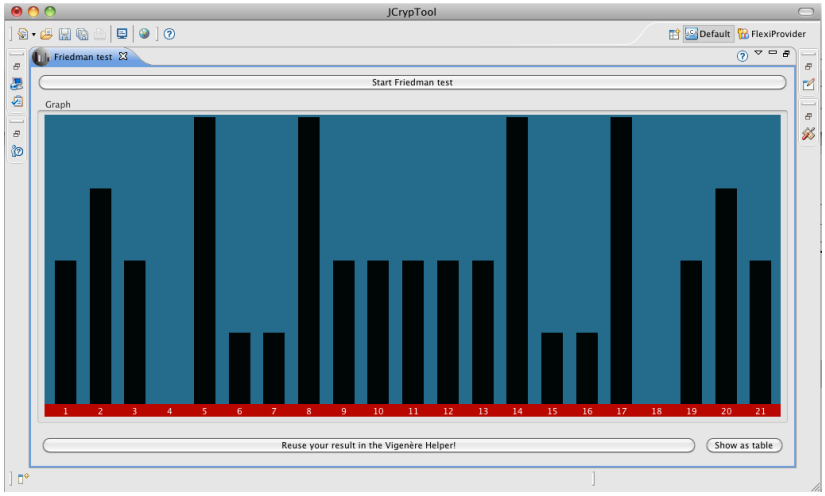


painel
lateral à direita oferece as opções de cifras clássicas, dentre as quais a ADFGVX. Nas abas inferiores é possível acessar as funções de criptoanálise.



De fato, o JCripTool não é uma ferramenta que irá reverter uma cifra qualquer - ainda que conhecida a criptografia - técnica de automática. As de forma para a ferramentas fornecidas são criptoanálise auxiliam o aquelas que no processo de criptoanalista em questão. vencer a cifra





Como pode ser notado nas figuras a seguir, é possível realizar de forma rápida uma estudo sobre a frequência dos caracteres ou um Teste de Friedman.

Contudo, não há nenhum opção que permita tratar a cifra ADFGVX de forma mais vertical. A ADFGVX é imune à ataques de análise de frequência devido à sua dupla transposição com a palavra-chave, de maneira que o JCripTool apenas oferece, com o suas opções de hoje, um conjunto insuficiente de ferramentas, que não permitem fazer deduções mais precisas sobre uma criptografia do tipo ADFGVX.

Referências

1. **ADFGVX Cipher** - *Wikipedia, the Free Encyclopedia*
   http://en.wikipedia.org/wiki/ADFGVX_cipher - Acessado em 07/12/2010

2. **Singh, Simon** - *O Livro dos Códigos, a Ciência do Sigilo*
   Editora Record, 2001.

3. *Encryption Pages - ADFGVX Cipher*
   http://courses.gdeyoung.com/pages.php?cdx=170 - Acessado em 07/12/2010

4. JCripTool Homepage
   http://jcryptool.sourceforge.net/JCrypTool/Home.html