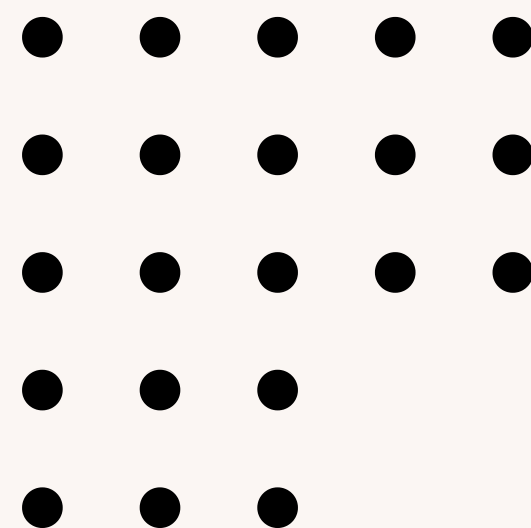


EXTENSÃO DA CIFRA DE CÉSAR: IMPLEMENTAÇÃO DE CIFRAS BASEADAS EM CHAVES NUMÉRICAS VARIÁVEIS

Arthur Monteiro Pereira

Filipe Brinati Furtado



TÓPICOS DE ABORDAGEM

- Criptografia
- Cifra de Cesar
- Trabalhos Relacionados
- Modificações
- Resultados



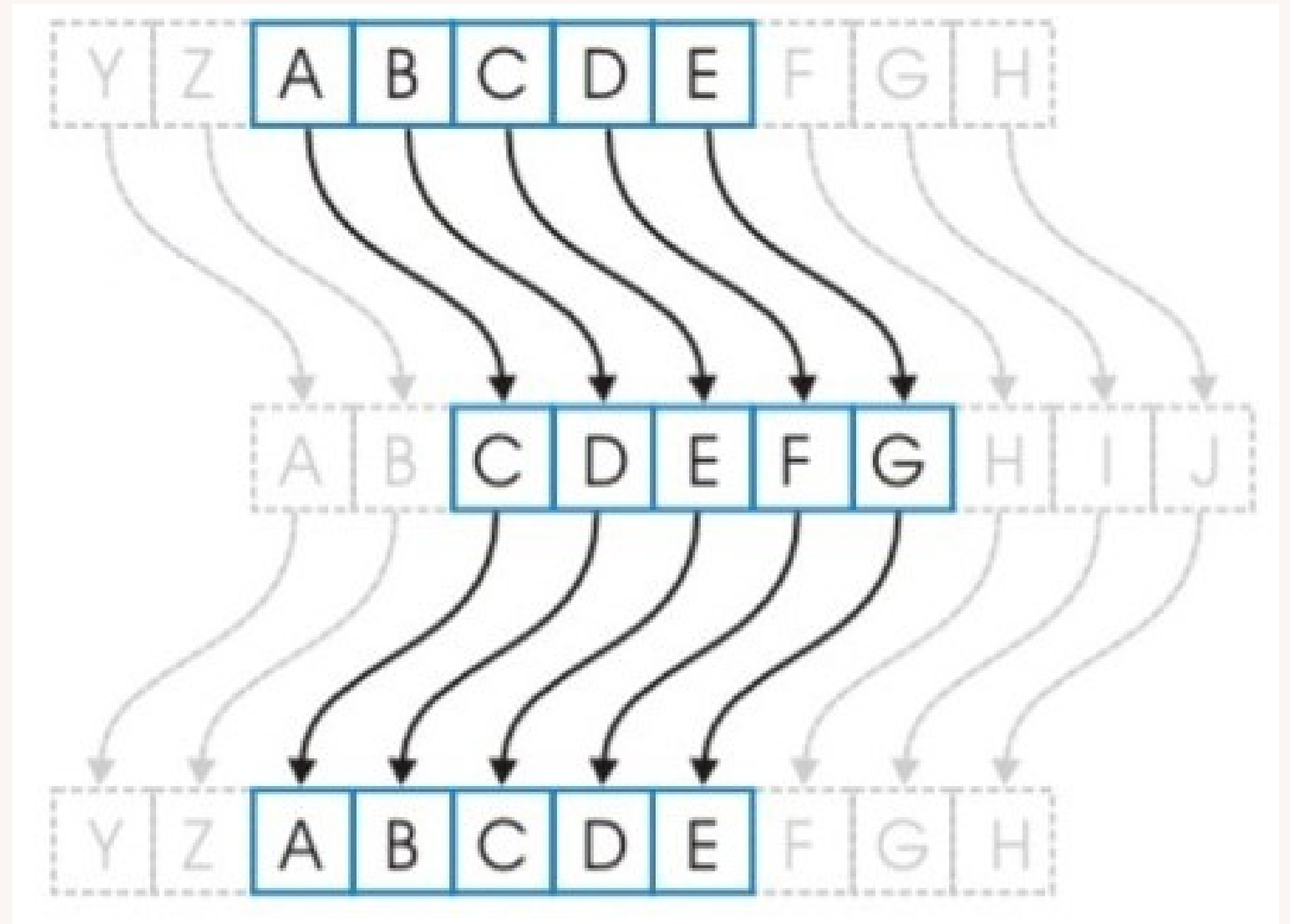
CRIPTOGRAFIA

A arte e a ciência de criar dados não legíveis ou cifras, de forma que apenas a pessoa pretendida seja capaz de decifrar e ler os dados.



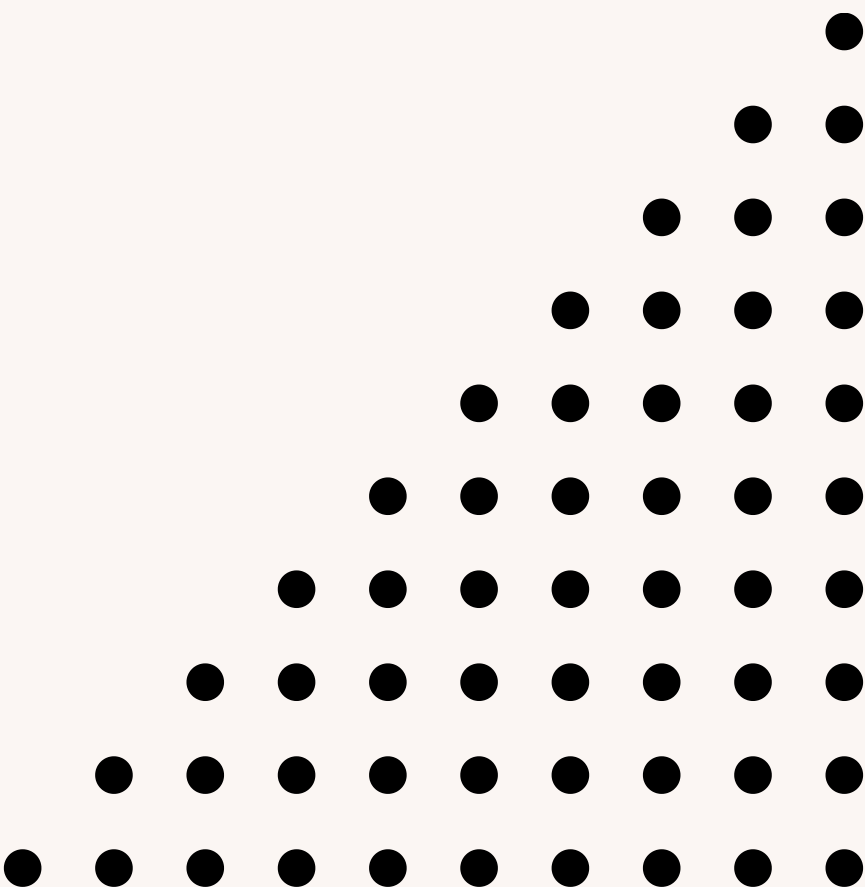
CIFRA DE CÉSAR

- Tipo de cifra de substituição monoalfabética;
- Vulnerável a ataques de força bruta;
- Limitada ao alfabeto;
- Suscetível a ataques de análise de frequência;





TRABALHOS RELACIONADOS

- 1 Modificação César dinâmica
 - 2 Transposição multinível segura
 - 3 Combinação César-Vigenère
 - 4 César com troca de chaves
 - 5 Cifra legível monoalfabética
- 

CIFRA AF

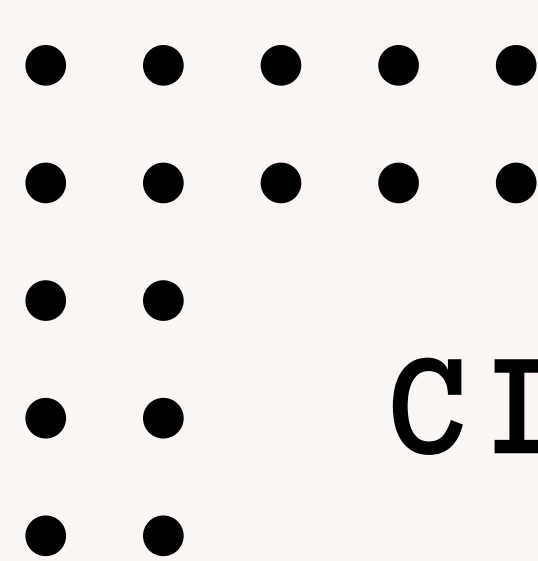
- Tipo de cifra de substituição baseado em deslocamento
- Utiliza caracteres imprimíveis tabela ASCII com alfabeto
- Vulnerável a ataques de força bruta;
- Resistente a ataques de análise de frequência;
- Rotação definida por caractere a caractere da chave

Origem:AABBCDEF
chave:1 2 3

Destino :

Rotação:

B	C	E	D	F	H	G
1	2	3	1	2	3	1



CIFRA AF2

- Tipo de cifra de substituição baseado em deslocamento
- Utiliza caracteres imprimíveis tabela ASCII com alfabeto
- Vulnerável a ataques de força bruta;
- Resistente a ataques de análise de frequência;
- Rotação definida por par de caractere a par de caractere da chave

Origem:AABCDEF

chave:1 2 3

Destino:

M	`	Y	O	c	\	R
1 2	3 1	2 3	1 2	3 1	2 3	1 2

Rotação:

RESULTADOS

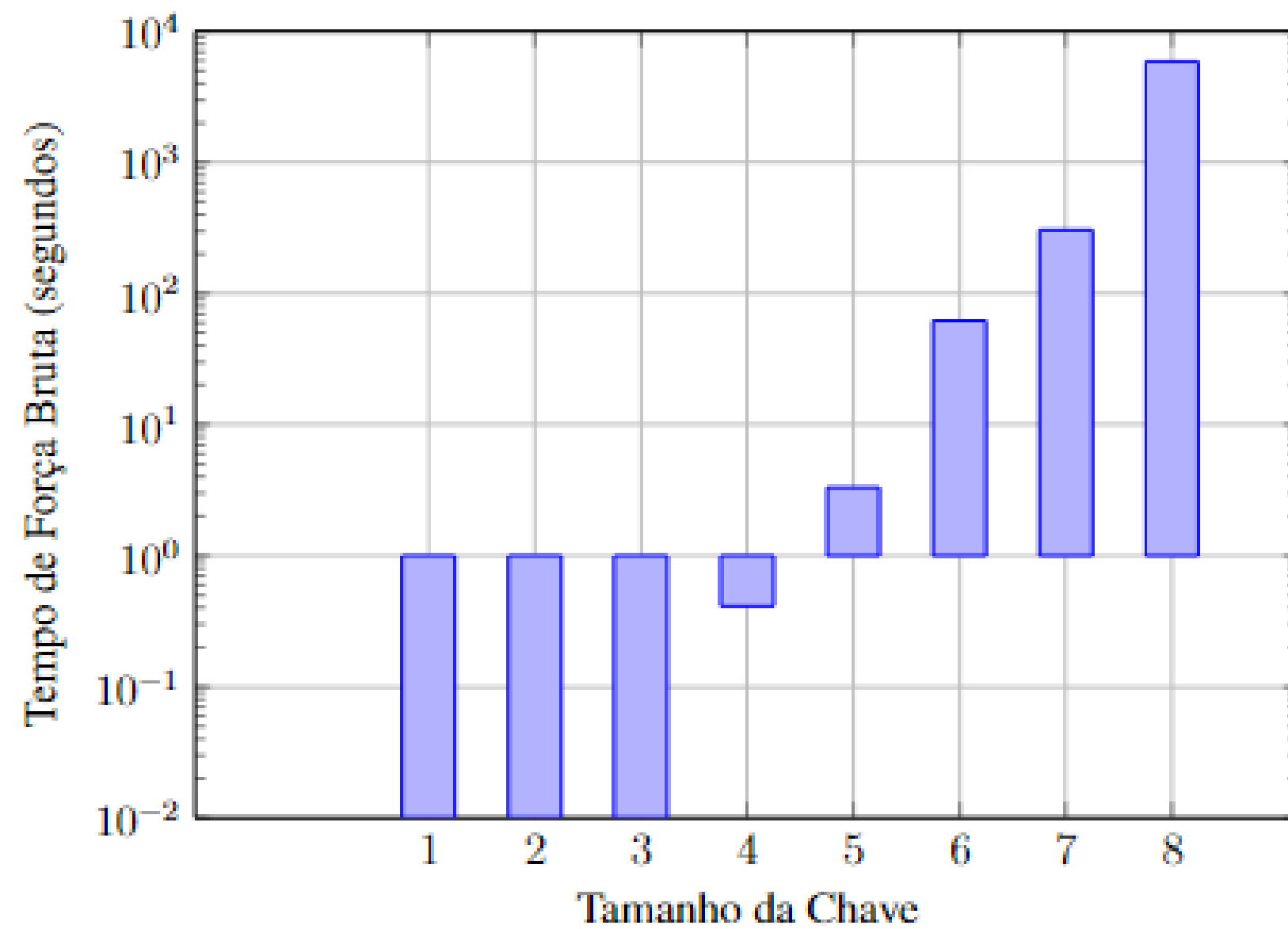
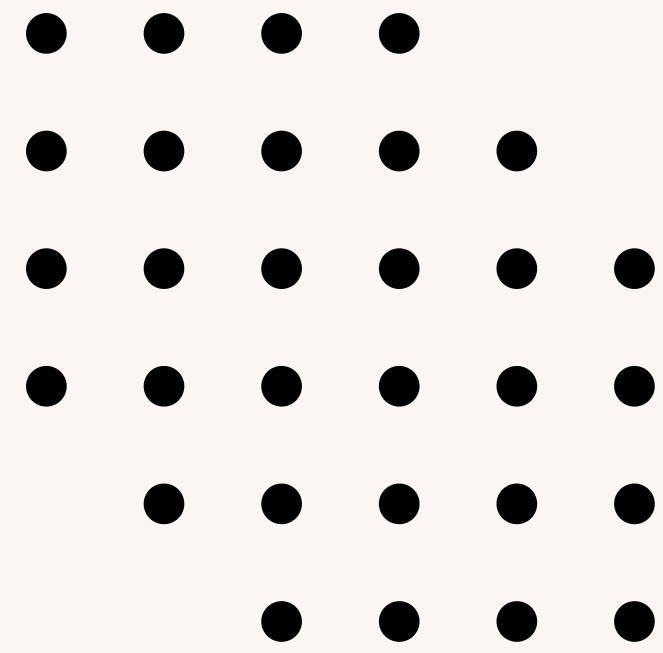


Figura 1. Tempo de força bruta para diferentes chaves em escala logarítmica

AMEAÇAS À VALIDADE

- Desempenho do Hardware
- Algoritmos de Força Bruta
Otimizados





REFERÊNCIAS

- Gowda, S. N. (2016, September). Innovative enhancement of the Caesar cipher algorithm for cryptography. In 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall) (pp. 1-4). IEEE.
- Goyal, K., & Kinger, S. (2013). Modified caesar cipher for better security enhancement. International Journal of Computer Applications, 73(3), 0975-8887.
- Mishra, A. (2013). Enhancing security of caesar cipher using different methods. International Journal of Research in Engineering and Technology, 2(09), 327-332.
- Omolara, O. E., Oludare, A. I., & Abdulahi, S. E. (2014). Developing a modified hybrid caesar cipher and vigenere cipher for secure data communication. Computer Engineering and Intelligent Systems, 5(5), 34-46.
- Purnama, B., & Rohayani, A. H. (2015). A new modified caesar cipher cryptography method with legible ciphertext from a message to be encrypted. Procedia Computer Science, 59, 195-204.
- Terada, R. (2008). Segurança de dados: criptografia em rede de computador. Editora Blucher.