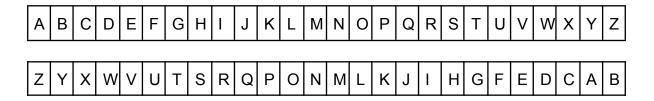
#### NOMES:

ANDREY FERREIRA PICHUTI / RA: 82414002 MOSHE ACHKIY SILVERIO MANDUJANO / RA: 824115318 JOÃO GABRIEL SILVA BARBARA DA CONCEIÇÃO / RA: 82415176 NICOLAS TRINDADE MARCIANO / RA: 824135758

#### CRIPTOGRAFIA

# **EXEMPLOS HISTÓRICOS DE CRIPTOGRAFIAS**

**Atbash:** A Cifra Atbash é uma das mais antigas cifras conhecidas, foi bem utilizada por escribas hebreus para codificar mensagens na Bíblia. É uma cifra de substituição simples, que consiste em trocar a letra do alfabeto pela correspondente na ordem inversa.



JN-25: A Cifra JN-25 foi um tipo de criptografia criada pela marinha japonesa durante a Segunda Guerra Mundial. De acordo com a NSA, "O JN-25 consistia em um livro de códigos com aproximadamente 27.500 entradas e um livro aditivo para super encriptar os valores do livro de códigos. O livro aditivo consistia em 300 páginas, cada página contendo 100 grupos aleatórios de cinco dígitos. Deve-se notar que este livro aditivo para o JN-25 não era um bloco de uso único: os grupos de cinco dígitos eram reutilizados, conforme necessário."

# **CRIPTOGRAFIAS SIMÉTRICAS**

Chamamos uma criptografia de simétrica quando as duas chaves, tanto a do remetente, quanto a do destinatário, são privadas. Essas chaves também são iguais, por isso simétricas, o que quer dizer que a mesma chave que cifra a mensagem para enviar (remetente) é a que decifra para receber (destinatário). A seguir vamos ver dois exemplos de algoritmos de chaves simétricas.

**RC2:** criado por Ron Rivest, foi desenvolvida principalmente para ser utilizada em criptografia de e-mail corporativo. Seu tamanho é variável, podendo alcançar até 1024 bits. Vale ressaltar que Ron Rivest, dono da RSA Data Security Inc. também criou o RC4, RC5 e RC6.

**CAST:** criado por Carlisle Adams e Stafford Tavares, o CAST é um algoritmo de cifra de bloco, com tamanho variável de 40 a 128 bits.

# **CRIPTOGRAFIAS ASSIMÉTRICAS**

Agora, uma criptografia assimétrica é caracterizada por chaves diferentes entre o remetente e o destinatário. O remetente pode utilizar uma chave pública, e assim, o destinatário usará uma chave privada, ou vice-versa. A seguir, vamos ver dois exemplos de algoritmos de chaves assimétricas.

<u>Curvas elípticas:</u> Neal Koblitz e V. S. Miller pensaram em uma nova forma de sistema criptográfico, utilizando curvas elípticas para a formação de um sistema criptográfico.

**<u>EIGamal:</u>** esse algoritmo utiliza o problema do logaritmo discreto para dar formação às suas chaves, ou seja, a segurança da chave se dá pela dificuldade de resolução do problema do logaritmo.