Explicação do método:

1 - Substituição de alfabetos:

Primeiro, cada letra da frase, ainda a ser escolhida, será substituída pela sua corresponde em uma versão alternativa do alfabeto (Figura 1). A palavra “casa”, por exemplo, será então reescrita como:

'C' → 'A'
'A' → 'B'
'S' → 'O'
'A' → 'B'

A	**Bê (B)**	**Cê (C)**	**Dê (D)**	**E (E)**	**Éfe (F)**	**Gê (G)**	**Agá (H)**	**I (I)**	**Jota (J)**	**Cá (K)**	**Éle (L)**	**Eme (M)**
A (A)	Agá (H)	Bê (B)	Cá (K)	Cê (C)	Dablio (W)	Dê (D)	E (E)	Efe (F)	Ele (L)	Eme (M)	Ene (N)	Erre (R)
Ene (N)	**O (O)**	**Pê (P)**	**Quê (Q)**	**Érre (R)**	**Ésse (S)**	**Tê (T)**	**U (U)**	**Vê (V)**	**Dablio (W)**	**Ípsilon (Y)**	**Xis (X)**	**Zê (Z)**
Esse (S)	Gê (G)	I (I)	Ípsilon (Y)	Jota (J)	O (O)	Pê (P)	Quê (Q)	Tê (T)	U (U)	Vê (V)	Xis (X)	Zê (Z)

Figura 1 - Alfabeto alternativo.

2 - Uso do RSA:

Para deixar mais segura a frase recém cifrada e descrita no item 1, será utilizado o algoritmo RSA, por meio de sua chave pública. Dessa maneira, quando o destinatário receber a mensagem codificada, poderá decifrá-la utilizando sua chave privada RSA.

Linguagem de Programação: Python.

Tamanho da senha: A ser definida pelo RSA, tendo como padrão 2048 bits e no máximo 4096 bits.

Quantidade de Senhas: Chave privada e pública do RSA.

Algoritmos de cifragem utilizados: Método criado por mim em que faz substituições alfabéticas (simétrico) e o algoritmo RSA (assimétrico).

Sua contribuição, por exemplo, o que você colocou de diferente no conjunto de algoritmos. Por que você acha que o seu algoritmo proposto é mais seguro que apenas utilizar cifras originais? Explique.

Propus implementar um sistema de substituição alfabética, onde realiza a troca das letras por outras que foram reordenadas em ordem alfabética (Figura 1). Acho que meu algoritmo, apesar de simples, é válido e bem aplicado, pois não possui um padrão como a cifra de César, que apenas desloca a posição do alfabeto, mas substitui as letras por sua correspondente de um segundo alfabeto aleatório, além de ter baixo risco de erros de código e compilação.