¿Por qué el cifrado César es inseguro hoy en día?

Por que el cifrado cesar ya es muy conocido y son muy reducidas las posibilidades (25)
no tienen mas posibilidades de hacer otros intentos y es fácil al atacante hacerlo por fuerza bruta descifrarlo en cuestión de minutos.

¿Cómo mejorarías este algoritmo para hacerlo más robusto?

1. Seria implementar más parámetros de símbolos
2. Ampliar el desplazamiento (clave) para tener menor posibilidad
3. Tener una carácter random en vez de tener todo en un solo orden