Sistema de Geração de Senhas Aleatórias a Partir de Sequências Humanas de Teclas

Resumo

Este documento apresenta um sistema inovador de geração de senhas que utiliza entradas humanas aleatórias por meio de teclado (ex: ABNT2) como fonte de entropia. A proposta se baseia no comportamento naturalmente caótico e imprevisível do ser humano ao interagir com um teclado, garantindo assim uma aleatoriedade genuína e não replicável por algoritmos tradicionais. O sistema aplica transformações sobre a sequência original (como inversão e combinações), gerando múltiplas variações e uma senha final altamente segura.

Contexto

A maioria dos sistemas atuais de geração de senhas se baseia em algoritmos pseudorrandômicos, que, embora eficazes, são determinísticos e previsíveis caso a semente seja comprometida. Por outro lado, o comportamento humano oferece uma fonte rica e autêntica de imprevisibilidade que ainda não foi plenamente explorada como mecanismo de geração de senhas.

Objetivo

Desenvolver uma plataforma que:

1. Capture sequências de teclas digitadas livremente por usuários humanos, garantindo que todas as teclas do teclado sejam pressionadas ao menos uma vez.
2. Aplique transformações sobre a sequência original:
   - Versão normal
   - Espelhada (reversa)
   - Combinações entre as duas (normal+espelhada, espelhada+normal)
3. Gere uma senha final com base em hash ou codificação derivada das sequências (ex: SHA-256).
4. (Opcional) Armazene anonimamente as sequências para formar um banco coletivo de entropia.

Funcionamento do Sistema

1. Input livre humano:

- Interface com teclado virtual (ou físico).
- Usuário pressiona teclas de forma totalmente livre e desestruturada.
- Requisito: todas as teclas devem ser pressionadas ao menos uma vez.

2. Geração das variações:

- A sequência é salva como S.

- Geração de S' = reverso(S).

- Montagem de variações: V1 = S, V2 = S', V3 = S + S', V4 = S' + S

3. Conversão em senha final:

- Aplica-se um hash (ex: SHA-256).

- Hash pode ser convertido para formatos como Base64 ou alfanumérico.

Diferenciais da Solução

- Utiliza aleatoriedade humana real, não simulada.

- Impossível de ser replicada por máquinas.

- Sistema aberto, transparente e auditável.

- Pode servir como camada adicional de segurança para gestores de senha, carteiras digitais ou autenticação.

Aplicações Possíveis

- Geração de senhas mestres únicas

- Criação de chaves para carteiras blockchain

- Autenticação offline

- Fonte de entropia distribuída

- Educação em segurança digital

Estado Atual da Invenção

Em fase conceitual e de documentação. Protótipo visual ou funcional ainda não implementado, mas em planejamento para desenvolvimento em ambiente web acessível.

Autor

Nome: Nicholas Centeno Ferreira

E-mail: Nicholas.C.Ferreira@hotmail.com

Data: 05/04/2025

Assinatura: