達磨さんが転んだ

目的

証憑もしくは暗号資産の基礎と材料を提供する。

形式

3の整数倍の行数からなる。1行目にデータ、2行目に年月日時刻、3行目にMD5ハッシュを記入。

連鎖

1行目のデータと2行目の時刻からハッシュを計算し3行目とする。
3行目のハッシュも加味して、後続の3n行を繰り返し計算・記録する。

データ

db.txt フアイルに保存する。

記録

darma.cgi を実行する。

検証

kensho.cgi を実行する。

問題

ローカル保存の場合はiterationを後から捏造できる。

対策

サーバーにデータを保存して、サーバーにログオンしてデータを入力する。入力データの制限。
SQL注入からサーバーを保護する。ハッシュ値は複数のサーバーに分散保存して、けん制する。
提供者はサーバーを監視する必要がある。電子証明書も絡めた対策・難読化が必要かもしれない。

類似

InternetProtocolのパケットに似ている。データと辿ったスイッチのIPを順繰りに付加していく。到達かTTLが0になるまで繰り返す。IPは実際にはSendmailのようにヘッダを付加していく方法しかない。
L2/L3スイッチを通る度にトンネル(ヘッダ付加と隠ぺい)するように。可変長のパケットは通らない。
スイッチングハブ2台で終わりの小規模LANでした(仕様書通り)。