mnemonic.js

Memorable & strong passphrases in the browser

Yiorgis Gozadinos, Crypho AS

ggozad@crypho.com, @ggozad
crypho.com

Private and secure real-time team collaboration.
We need to generate passphrases!

Log in

Email address

Security code
Send code via SMS
Enter the security code, from text message, or from the authenticator app. If you need a new code, click Send code via SMS

Passphrase

or, register a new account

Login
Enter mnemonic.js!

STRONG & MEMORABLE PASSPHRASES

- No obscure rules requiring special symbols, numbers or length.
- Using memorable native-language words (n=1626).
- Generated from random 32-bit integer sequences (3 words/integer).
Examples

• 32-bit
  confidence ourselves insult
  decimal: 652372173
  hex: 26e268cd

• 96-bit
  mean yesterday gone size
  waist lace endless apple
  war
  decimal: 24224384090962230467342891306
  hex: 4e45f0dced5ec11c772ff92a

• ~10.6bits/word
  Compare to:
  ~6.5bits/char for all ASCII and
  ~2bits/char for English words.
How does it work?

- encoding:

  \[
  \begin{align*}
  w[i,1] &= x \mod n, \\
  w[i,2] &= (x / n + w[i,1]) \mod n, \\
  w[i,3] &= (x / n^2 + w[i,2]) \mod n,
  \end{align*}
  \]

- decoding

  \[
  \begin{align*}
  w[i,1] &= \text{dict.indexOf}(\text{word}[i,1]) \\
  w[i,2] &= \text{dict.indexOf}(\text{word}[i,2]) \\
  w[i,3] &= \text{dict.indexOf}(\text{word}[i,3]) \\
  x &= w[i,1] + \\
      & \quad n((w[i,2] - w[i,1]) \mod n) + \\
      & \quad n^2 ((w[i,3] - w[i,2]) \mod n)
  \end{align*}
  \]
How do I use it?

Create a new mnemonic

```python
>>> m = new Mnemonic(96);
>>> m.toWords();
"grey", "climb", "demon", "snap", "shove", "fruit", "grasp", "hum", "self"
```

get the random UInt32 sequence or the hex

```python
>>> m.random
[174975897, 171815469, 1859322123]
>>> m.toHex();
"0a6deb990a3db22d6ed3010b"
```

or reconstruct it from its words

```python
>>> m = new Mnemonic(["grey", "climb", "demon", "snap", "shove", "fruit", "grasp", "hum", "self"]) ;
>>> m.toHex();
"0a6deb990a3db22d6ed3010b"
```
Contact

- Github: https://github.com/ggozad/mnemonic.js
- Crypho: http://crypho.com
- Twitter @ggozad
- ggozad@crypho.com