rance: Memorable Keys and Passwords

WIPS 2020 Flash Talk

Leah Namisa Rosenbloom
Brown University
leah_rosenbloom@brown.edu

rance: Memorable Keys and Passwords

- Essential Question: How can we achieve strong yet memorable passwords?
- Use Cases: protect info or generate cryptographic keys regardless of device access
  - Activists, dissidents, journalists, leakers, immigrants, and minorities
  - Devices seized or destroyed; surveillance, prosecution, detainment based on digital activity & comms
  - Need passwords strong enough to protect cryptographic keys, hide info/authenticate to peers
- Diceware (1995): pass-phrase of random words from a dictionary
  - Random words are easier than random alphanumeric strings; lots of random words also hard
- rance: pass-sentence of random words from various libraries
  - Added structure increases memorability; lots of structures, word combos increases randomness
  - 45 unique sentence structures, 14 simple (ex. N + V); 31 complex (ex. A + N & A + N + V)
  - Basic Strength (47 bits entropy), Extra Strength (79 bits), Symmetric-key Strength (132 bits)

rance Password (132.0 bits entropy)	**Diceware Password** (129.0 bits entropy)	**Alpha-Numeric Password** (131.0 bits entropy)
What majority of shrines speak, meanwhile gender kills unsparingly?	pep baste bad lark swan apple punch scab titan eyes	MlcGjYkvqa9HSeeuMkMbZd

- Next Steps: cryptographic key generator, platform integration