Admin:
- Pset #2 due today
- Pset #3 going out late - today
- Projects

Today:
- Stream ciphers
  - Definitions
  - Spritz (RC4)
  - ChaCha

Reading:
- Katz/Lindell §3.3.1

Project Ideas:
- Evaluate security of Whisper Systems product(s)
  (which are open source)
Recall OTP

\[ \text{pad} \rightarrow \text{cipher text} \]

How to generate a good pseudo-random pad

- "key" or "seed"
- \[ \{0,1\}^n \]
- Pseudo-random generator
- \[ \{0,1\}^{\ell(n)} \]
- \( \ell(n) > n \)

\[ G \]

\[ \text{pad} \]

G is secure if

\[ \begin{align*}
\text{Adv can not distinguish (in PPT) between} \\
\text{string } x \text{ drawn from } \{0,1\}^{\ell(n)} \text{ at random} \\
\text{result of } s \leftarrow \{0,1\}^n; \text{ output } G(s) \\
\text{with probability better than } \frac{1}{2} + \text{negl}(n)
\end{align*} \]
Stream cipher is a PRG with variable/arbitrary length output. API may be different:

- may distinguish long-term key from per-message key (nonce)
- may be counter-based

E.g., AES in CTR mode, ChaCha

or state-based

if next-state-fn is one-way
then shift of state won't enable reading past traffic
Spritz (BRCY) - seq slides
ChaCha — designed by Dan Bernstein

- chosen by google to replace RC4 in OpenSSL

- 512 bits

- output

- 512 block is 4 x 4 x 32

- 0, 1, 2, 3

- 4, 5, 6, 7

- 8, 9, 10, 11

- 12, 13, 14, 15

\[ QR = \text{quarterround} \] (inside 4 regs a, b, c, d e.g. one column):

\[ \begin{align*}
    a &= b; \\
    b &= c; \\
    c &= d; \\
    d &= a;
\end{align*} \]

\[ d \lll = 16 \]

\[ c \lll = 12 \]

\[ a \lll = 8 \]

\[ c \lll = 7 \]

ARX
add
rotate
XOR
instructions only

\( \text{key} \)

\( \text{nonce (index)} \)
double-rounds:

\[ QR (0, 4, 8, 12) \]
\[ (1, 5, 9, 13) \]
\[ (2, 6, 10, 14) \]
\[ (3, 7, 11, 15) \] \{ rows \}

\[ QR (0, 5, 10, 15) \]
\[ (1, 6, 11, 12) \]
\[ (2, 7, 8, 13) \]
\[ (3, 4, 9, 14) \] \{ diagonals \}

\[ Ch_4 Ch_4 = 10 \text{ double-rounds} \]