

Admin:

Pset #2 due today

Pset #3 going out later today

Projects

Today:

Stream ciphers

- Definitions
- Spritz (& RC4)
- ChaCha

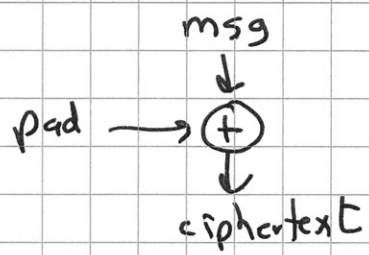
Reading:

Katz/Lindell §3.3.1

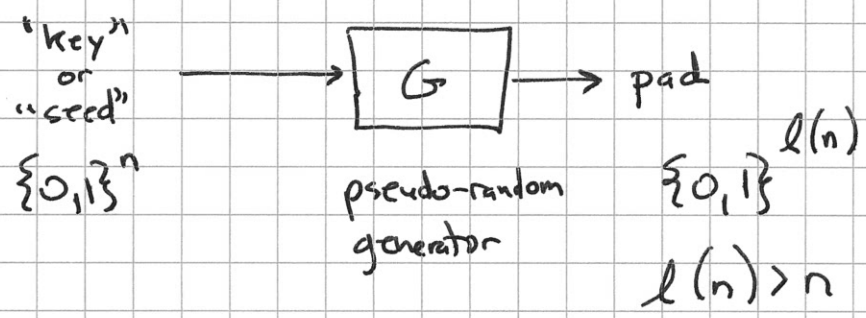
Project idea:

Evaluate security of Whisper Systems product(s)  
(which are open source)

Recall OTP



How to generate a good pseudo-random pad



G is secure if  
 aka  
 G is a pseudo-random generator

Adv can not distinguish (in PPT) between

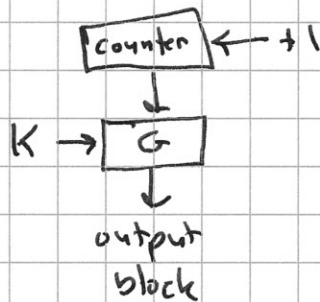
- string  $x$  drawn from  $\{0,1\}^{l(n)}$  at random
- result of  $s \leftarrow \{0,1\}^n$ ; output  $G(s)$

with probability better than  $1/2 + \text{negl}(n)$

Stream cipher is a PRG with variable/arbitrary length output. API may be different:

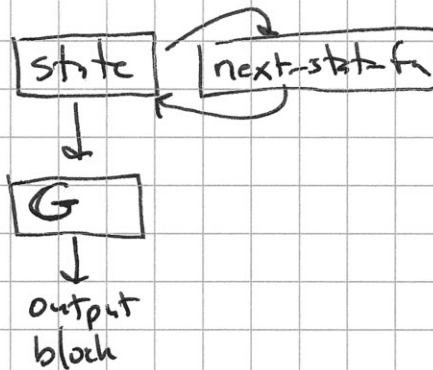
- may distinguish long-term key<sup>K</sup> from per-message key (nonce)
- may be counter-based

e.g. AES in CTR mode, ChaCha



← allows "random access" to portions of pad

or state-based



initial state is K

if next-state-fn is one-way then theft of state won't enable reading past traffic

TOPIC:

DATE: 3/9/15

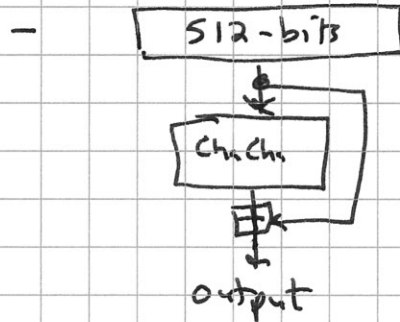
FILE UNDER:

PAGE: L10,4

Spritz (& RCY) - sec slides

ChaCha - designed by Dan Bernstein

- chosen by google to replace RC4 in openssl



- 512 block is 4x4x32

0,1,2,3

4,5,6,7

8,9,10,11

12,13,14,15

C	C	C	C
K	K	K	K
K	K	K	K
N	N	N	N

constant

} key

} nonce (index)

QR = quarterround (works on 4 regs a,b,c,d e.g. one column):

$a += b; d \wedge = a; d \lll = 16$

$c += d; b \wedge = c; b \lll = 12$

$a += b; d \wedge = a; d \lll = 8$

$c += d; b \wedge = c; b \lll = 7$

ARX  
add  
rotate  
XOR  
instructions  
only

double-round:

QR (0, 4, 8, 12)

(1, 5, 9, 13)

(2, 6, 10, 14)

(3, 7, 11, 15)

} rows



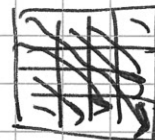
QR (0, 5, 10, 15)

(1, 6, 11, 12)

(2, 7, 8, 13)

(3, 4, 9, 14)

} diagonals



ChaCha20 = 10 double-rounds