Cryptographic competitions

D. J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

competitions.cr.yp.to

Related workshops:

Passwords13, Las Vegas,
30–31 July 2013:
passwordscon.org

DIAC 2013, Chicago,
11–13 August 2013:
2013.diac.cr.yp.to

CAESAR

"Competition for Authenticated Encryption: Security, Applicability, and Robustness"

competitions.cr.yp.to/caesar.html

Mailing list: crypto-competitions+subscribe@googlegroups.com

NIST is much too busy to run another competition but has generously provided a $333099 "Cryptographic competitions" grant to UIC.

Competition scheduling

AES schedule:

M0: 15 submissions.

M14: 5 finalists.

M28: 1 winner.

eSTREAM schedule:

M0: 34 submissions.

M11: 27 round-2 ciphers.

M24: 16 finalists.

M36: 8 portfolio ciphers.

M41: 7 portfolio ciphers.

SHA-3 schedule:

M0: 64 submissions.

M9: 14 round-2 functions.

M26: 5 finalists.

M48: 1 winner.

CAESAR schedule:

M0, 2014.01.15: submissions.

M11: round-2 candidates.

M23: round-3 candidates.

M35: finalists.

M47: portfolio.

CAESAR selection committee:

Steve Babbage
Daniel J. Bernstein
Alex Biryukov
Anne Canteaut
Carlos Cid
Joan Daemen
Christophe De Cannière
Orr Dunkelman
Henri Gilbert
Tetsu Iwata
Lars R. Knudsen
Stefan Lucks
David McGrew
Willi Meier
Kaisa Nyberg
Bart Preneel
Vincent Rijmen
Matt Robshaw
Phillip Rogaway
Greg Rose
Serge Vaudenay
Hongjun Wu

PHC

"Password Hashing Competition"

https://
password-hashing.net

Goals:
secure; **slow**;
better than MD5, SHA-1, SHA-2,
PBKDF2, bcrypt, scrypt.

Applications:
password hashing for web services;
key derivation for disk encryption;
PIN hashing for mobile platforms;
etc.

Committee:

Tony Arcieri
Jean-Philippe Aumasson
Dmitry Chestnykh
Jeremi Gosney
Russell Graves
Matthew Green
Peter Gutmann
Pascal Junod
Poul-Henning Kamp
Stefan Lucks
Samuel Neves
Colin Percival
Alexander Peslyak
Marsh Ray
Jens Steube
Steve Thomas
Meltem Sonmez Turan
Zooko Wilcox-O'Hearn
Christian Winnerlein
Elias Yarrkov