News

First cypto news since last Sept is SHA-3 winner Keccak. (Oct 2012. pending final standardization)

http://en.wikipedia.org/wiki/Sha-3 http://ehash.iaik.tugraz.at/wiki/Keccak
Underlying “sponge construction” can be used to build ciphers too.
Key besides speed/simplicity is invisible state affected only by permutation/diffusion, so opponent never sees full interior state.

SHA-3 – The New Hash Standard Hanno **Böck**

http://arstechnica.com/security/2013/07/crypto-flaw-makes-millions-of-smartphones-susceptible-to-hijacking/

Mobiles may be vulnerab
IBNLive-Jul 21, 2013
Cryptography allows co
network. Karsten Nohl,

Sim card flaws leave millions of mobile phones open to attack ...

The Guardian-2 hours ago
... can be run through with *cryptanalysis*. The resulting cryptographic key allows the hacker to send well-signed Java software to the sim card.

SIM card encryption exploit leaves mobile phone users vulnerable to ...
Inquirer-Jul 22, 2013
SIM Cards Cracked; Hundreds of Millions of Phones Vulnerable
Infosecurity Magazine-Jul 22, 2013
Another BYOD Worry: Hacking Via SIM-Card Vulnerability
Highly Cited -Forbes-Jul 22, 2013
'We become the SIM card': 750 million mobile phones could be ...
Blog -RT (blog)-Jul 22, 2013
all 148 news sources » has images !

Cryptopocalypse
http://www.technologyreview.com/news/517781/math-advances-raise-the-prospect-of-an-internet-security-collapse/

Ref
preso https://www.isecpartners.com/media/105564/ritter_samuel_stamos_bh_2013_cryptopocalypse.pdf

Math Advances Raise the Prospect of an Internet Security Crisis

MIT Technology Review - 40 minutes ago
Stamos called on the security industry to think about how to move away from on Diffie-Hellman and RSA, and specifically to use an alternative known as elliptic curve **cryptography** (ECC) that's significantly younger but relies on more intractable mathematical **...**

Black Hat 2013: Experts urge elliptical curve cryptography adoption
TechTarget - 57 minutes ago
The Diffie-Hellman scheme, first published in 1976, allows for secure exchange of secret keys -- a step critical for broad use of symmetric-key **cryptography** -- and is based on the computational difficulty of solving the discrete logarithm problem (DLP). The RSA **...**

Black Hat: Elliptical curve cryptography coming as smarter algorithms threaten ...
Network World - 9 hours ago
Network World - Las Vegas -- Within five years the math for cracking encryption algorithms could become so efficient that it may render today's commonly used RSA public key **cryptography** algorithm obsolete, Black Hat attendees were told. While it might take **...**

Crypto Gains Ramp Up Calls to Get Ahead of Inevitable RSA Algorithm Downfall
Threatpost - 4 hours ago
LAS VEGAS – **Cryptographic** breakthroughs have accelerated in the past six months in areas such as discrete logarithm computations that lead experts to believe that breaking the stalwart RSA algorithm may be in the not-too-distant future. A team of crypto **...**

Schneier on Cryptopocalypse “I don't see any reason to worry.”
http://www.schneier.com/blog/archives/2013/08/the_cryptopocal.html
& https://news.ycombinator.com/item?id=6237059

Commentary.

link Recent versions of SSH (6.1p1 on Ubuntu 13.04) support ECDSA, http://en.wikipedia.org/wiki/Elliptic_Curve_DSAUnfortunately, gnome-keyring-daemon can't deal with those keys.

(nor can GPG)

discrete logarithm problem (which you can learn about in this highly informative video) (khan academy)

ECC asymmetric is faster, shorter keys; scalable, not susceptible to factoring or discrete log improvements; but patent encumbered, and relatively young.

http://blog.cryptographyengineering.com/2013/08/is-cryptopocalypse-nigh.html (re peat)

> money grafs – “the payoff: all of the fields we use to implement most cryptography -- things like (non-elliptic-curve) DSA, Diffie-Hellman, and even the fields we use to implement NIST standard elliptic curves -- are prime fields and hence don't have the necessary properties [*i.e., small characteristic*] to make the Joux results meaningful. …
>
> “ … we should be switching to elliptic curve cryptography (ECC) as soon as possible, in part just so people can start using high-security cryptosystems

without paying performance and bandwidth through the nose for the privilege"

so Joux's result isn't dangerous in itself but is an example of unexpected leap forward that could be meaningful next time.
He notes the undeveloped PK Alternatives if Joux++ next result(s) applied to factoring, prime fields and ECC, aren't pretty.

- McEliece cryptosystem, McEliece and its modern variants are based on problems in algebraic coding theory. 2008 analysis Recent improvements – known NP-hard, quantum resistant, but keys are massive.
- Lattice-based cryptosystems. E.g. NTRU cryptosystem. "relatively well-studied" some standards.IEEE 1363.1 & ANSI X9.98-2010. Uh oh patent . Also quantum resistant.

Errata Security: Tor is still DHE 1024 (NSA crackable)

blog.erratasec.com/**2013**/09/tor-is-still-dhe-1tuch info on **Diffie-Hellman key** exchange **sizes**

CryptoCat – non-cryptographer fail. Again.http://nakedsecurity.sophos.com/2013/07/09/anatomy-of-a-pseudorandom-number-generator-visualising-cryptocats-buggy-prng/

http://www.securityorb.com/2013/08/blackhat-usa-2013-summary-part-1-3/

http://arstechnica.com/security/2013/07/hack-exposes-e-mail-addresses-password-data-for-2-million-ubuntu-forum-users/

http://arstechnica.com/security/2013/07/bad-kitty-rooky-mistake-in-cryptocat-chat-app-makes-cracking-a-snap/

(not the first iirc)

see also Here come the encryption apps!

http://www.schneier.com/blog/archives/2013/06/cracking_the_kr.html Kyptos Sculpture

The NSA cracked the Kryptos sculpture years before the CIA

Wired.co.uk-Jul 11, 2013
In 1991, while on a trip to the CIA, a group of NSA cryptanalysis "interns" diligently scribbled all the letters from the sculpture onto sheets of ...

BREACH.

http://arstechnica.com/security/2013/08/gone-in-30-seconds-new-attack-plucks-

secrets-from-https-protected-pages/
BREACH extends CRIME header compression oracle attack to a known but unexplored usecase on REPLY
https://news.ycombinator.com/item?id=6141862
http://arstechnica.com/security/2013/08/no-easy-way-to-stop-breach-from-plucking-secrets-from-https-pages-feds-say/
countermeasures -- The tactics, suggested by researchers Angelo Prado, Yoel Gluck, and Neal Harris, include the following:

- ❐Disable HTTP compression
- ❐Separate the secrets from the user input
- ❐Randomize the secrets in each client request
- ❐Mask secrets (effectively randomizing by XORing with a random secret per request)
- ❐Protect webpages from CSRF attacks
- ❐Obfuscate the length of Web responses by adding random amounts of arbitrary bytes

(self defense, use NOscript to defend against CSRF? https://www.google.com/search?q=NOscript+CSRF)
& https://blogs.akamai.com/2013/08/assessment-of-the-breach-vulnerability.html

Lucky 13 timing variant of BEAST Padding Oracle
http://arstechnica.com/security/2013/02/lucky-thirteen-attack-snarfs-cookies-protected-by-ssl-encryption/
http://www.isg.rhul.ac.uk/tls/Lucky13.html **CBC-mode encryption**
(only semi related http://www.isg.rhul.ac.uk/tls/ RC4 TLS WPA/TKIP)
http://en.wikipedia.org/wiki/Lucky_Thirteen_attack

http://arstechnica.com/security/2013/08/how-do-you-stop-https-defeating-breach-attacks-let-us-count-the-ways/ Goodin
http://nakedsecurity.sophos.com/2013/08/06/anatomy-of-a-cryptographic-oracle-understanding-and-mitigating-the-breach-attack/
https://blog.torproject.org/blog/hidden-services-current-events-and-freedom-hosting
https://www.djangoproject.com/weblog/2013/aug/06/breach-and-django/
Ø Comments https://news.ycombinator.com/item?id=6166292

Rails too https://news.ycombinator.com/item?id=6150535 &https://github.com/rails/rails/pull/11729 comments 2206, 2208

TLS Security:

- The TLS protocol is showing its age, but newer standards help. Article by Hanno **Böck** not online yet - Admin-Magazine.com issue#15 http://www.admin-magazine.com/Archive/2013/15
- **Attack of the week: RC4 is kind of broken in TLS** & **http://www.isg.rhul.ac.uk/tls**

(only semi related http://www.isg.rhul.ac.uk/tls/ RC4 TLS WPA/TKIP)

How to 'backdoor' an encryption app

http://blog.cryptographyengineering.com/2013/06/how-to-backdoor-encryption-app.html

Related http://www.wired.com/threatlevel/2013/08/freedom-hosting/

The Ideal Cipher Model (wonky)

CRYPTO
(See SN above) The Telnet-pocalypse - Gibson Research Corporationhttps://www.grc.com/sn/sn-396.pdf 1.2M routers and HP printers w/ default (or null) password telnet exposed to internet side.

Tor backdoor

https://www.cryptocloud.org/viewtopic.php?f=9&t=2894&p=3852#p3852
http://arstechnica.com/tech-policy/2013/08/researchers-say-tor-targeted-malware-phoned-home-to-nsa/
http://blogs.computerworld.com/tor-onion-router-nsa-fbi-child-porn-22598-itbwcw
http://www.schneier.com/blog/archives/2013/08/has_tor_been_co.html

bgp.

http://www.zdnet.com/bgp-spoofing-routing-router-phishing-why-nothing-on-the-internet-is-actually-secure-7000019015/

Other
Crypto Animations&diagrams

https://www.google.com/search?q=cryptography+animation
http://www.discourse.net/2009/09/aes_explained_in_a_cartoon/
> http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html (links to PDF and PPT versions CC-BY)
& There are ECC **animations** on youtube

PuTTY 0.63 released, fixing four security holes (greenend.org.uk) 8 points by bwblabs33 minutes ago | discuss

Twitter’s New Two-Factor Solution Kicks SMS to the Curb (wired.com) 82 points bykylerandolph 2 hours ago | 42 comments
Uses RSA2048

One-Time Pad visualized with XOR, AND, and OR - Imgur = bit.ly/xorxor(http://twit.tv/show/security-now/392 https://www.grc.com/sn/sn-392.pdf or .txt)

imgur.com/a/yjhTo
image of Charles Babbage. View full resolution · Download full resolution · Charles Babbage **...** Charles Babbage; One-Time Pad with XOR; One-Time Pad with AND.

Steve, I like this because it is so clear. It just says - so what they did was they took pseudorandom noise, and they XORed the noise with the picture, or they ORed the noise with the picture, or they ANDed the noise with the picture.

Compare with http://en.wikipedia.org/wiki/File:Tux_ecb.jpg !

Vernam's co-author, Mauborgne broke Plaifair. Do I have, can I find his 19pp pamphlet?

Practical uses of the wave meter in wireless telegraphy : Mauborgne ...

- **Article - Central Washington Universitywww.cwu.edu/~boersmas/Ciphers/Cowan_article.pdf Jan 10, 2008 - The reader will now appreciate why Mauborgne's methods for solving Playfair, developed on a message of 800 letters, will usually be useless** ... // Simulated Annealing attack. Not Mauborgne – which requires long messages. //

How to identify and break Playfair < .DOC ! www.ling.ohio-state.edu/~cbrew/2008/winter/294L/playfair **The Playfair cipher is a simple but effective cipher that was actually invented not by ... in 1854 and Joseph Mauborgne'spublication of a method for its solution.**

PLAYFAIR - cryptospecs cryptospecs.googlecode.com/svn/trunk/classical/specs/playfair**.pdf**

Military Communications: From Ancient Times to the 21st Century - Page 282 - Google Books Result books.google.com/books?isbn=1851097325Christopher H. Sterling - 2008 - History Mauborgne, Joseph Oswald As the German right wing advanced across ... In 1914, he was the first to solve thePlayfair complex field cipher system then used by .

Playfair Cipher Explained - YouTube

PGP –

- https://en.wikipedia.org/wiki/Pretty_Good_Privacy & http://www.gnupg.org/

Trivia – media references.

- GK/PHC Lake Woebegone
- SNL Bass-O-matic. http://en.wikipedia.org/wiki/BassOmatic "there is no published cryptanalysis ofBassOmatic," but was considered weak http://osvdb.org/show/osvdb/45179 "Multiple Unspecified Cryptanalysis Weaknesses" apparently including intrinsic susceptibility tohttp://en.wikipedia.org/wiki/Differential_cryptanalysis (in addition to repairable glitches)
  q.v. PGP book

Cryptanalysis pdf

GPG https://www.google.com/search?q=gpg http://irtfweb.ifa.hawaii.edu/~lockhart/gpg/ CheatSheet

TWIT Know How #50 (HD SD –L SD-small Audio)
June 27th, 2013
Episode #50: Encrypt your email with PGP
Shannon Morse came by to help us make our mail more secure. Find out how easy it is to encrypt your email using PGP.

Twit.tv/sn August 21, 2013 **#418: Considering PGP** “Steve and Leo cover the consequences of the Snowden leaks and, with that in mind, they examine the Pretty Good Privacy (PGP) system for encrypting email and attachments.”

How to secure and encrypt your OS X Mail messages with**GPGMail 2** (imore.com)

- **hpr0222 :: Alpine GPG - Hacker Public Radio**

  hackerpublicradio.org/eps.php?id=0222
  Nov 5, 2008 - Filed under Episode | Comments (0). For more info on PGP andGPG: The Bad Apples episode 2x04 ogg · The Bad Apples episode 2x04 mp3

- **0441 - Migrating Your GPG Key and Starting GPG-Agent**

  hackerpublicradio.org/eps.php?id=0441
  Sep 9, 2009 - Hacker Public Radio is an podcast that releases shows every weekday Monday through Friday. Our shows are produced by the community **...**

- **0443 - How to Sign C Files with GPG - Hacker Public Radio**

  hackerpublicradio.org/eps.php?id=0443
  Sep 11, 2009 - Hacker Public Radio is an podcast that releases shows every weekday Monday through Friday. Our shows are produced by the community **...**