

GOOG 13

.

|

|

|



JAVA CRYPTOGRAPHY DEEP DIVE: TAMING THE BEAST

@ABSTRACTJ



open source



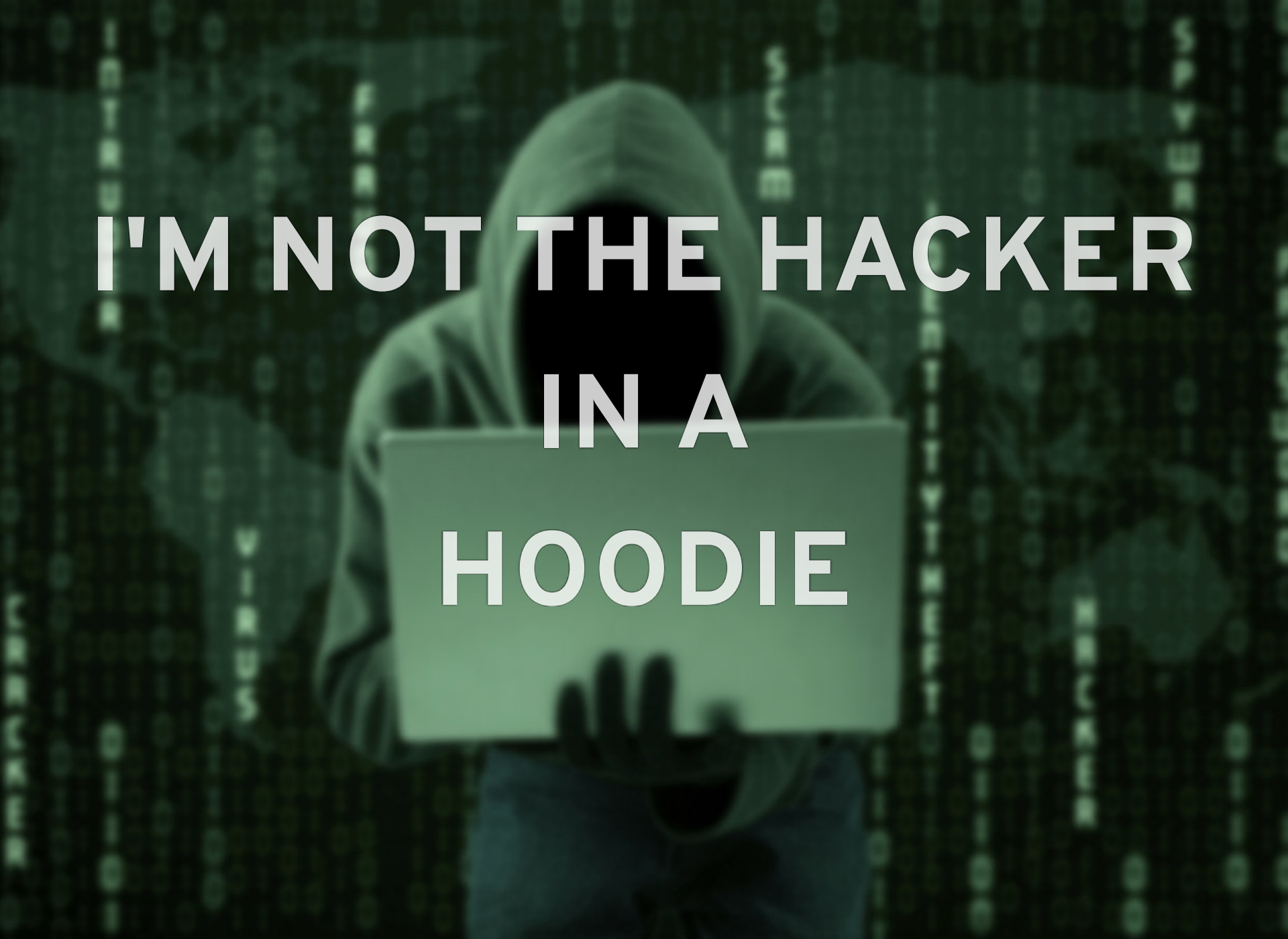
redhat.



AeroGear

The background of the image features a gradient of colors from purple at the top to orange and yellow at the bottom, resembling a sunset. In the center, two black silhouettes of hands are positioned to form a heart shape. The text "SECURITY & CRYPTOGRAPHY" is overlaid on this graphic in a white, bold, sans-serif font. The word "SECURITY" is at the top, "&" is in the middle, and "CRYPTOGRAPHY" is at the bottom.

SECURITY & CRYPTOGRAPHY

A person wearing a dark hoodie is holding a laptop in front of their face. The background is dark with vertical columns of green, glowing characters, reminiscent of the 'Matrix' digital rain effect. The text 'I'M NOT THE HACKER IN A HOODIE' is overlaid in large, white, bold, sans-serif capital letters.

**I'M NOT THE HACKER
IN A
HOODIE**

**I'M ONLY VERY,
VERY CURIOUS**



DISCLAIMER

**SECURITY IS ABOUT
FEELING VS REALITY**



The image features a perspective view of a tunnel formed by concentric, glowing blue rings of binary code (0s and 1s). The rings curve inward, creating a sense of depth and leading the eye toward a bright, white light source at the far end of the tunnel. The overall color palette is a vibrant blue, with the white light providing a strong contrast. Centered across the middle of the image is a dark, semi-transparent rectangular box containing the word "CRYPTOGRAPHY" in a bold, white, sans-serif typeface.

CRYPTOGRAPHY

The study of codes, or
the art of writing and
solving them.

Oxford Dictionaries



WHAAAAAT ?!

memegenerator.net

Cryptography is the
art and science of
encryption

Cryptography Engineering



WHAAAAAT ?!

memegenerator.net

The background features a grayscale image of classical stone columns. Overlaid on this are red geometric shapes: a large triangle in the top-left and bottom-right corners, and a series of concentric squares forming a pattern in the bottom-right area.

HISTORICALLY FOCUSED ON SECRET COMMUNICATIONS

VIGENÈRE CIPHER

~ 1553, Rome

k = j a v a a o e

m = m o r n i n g

mod 26

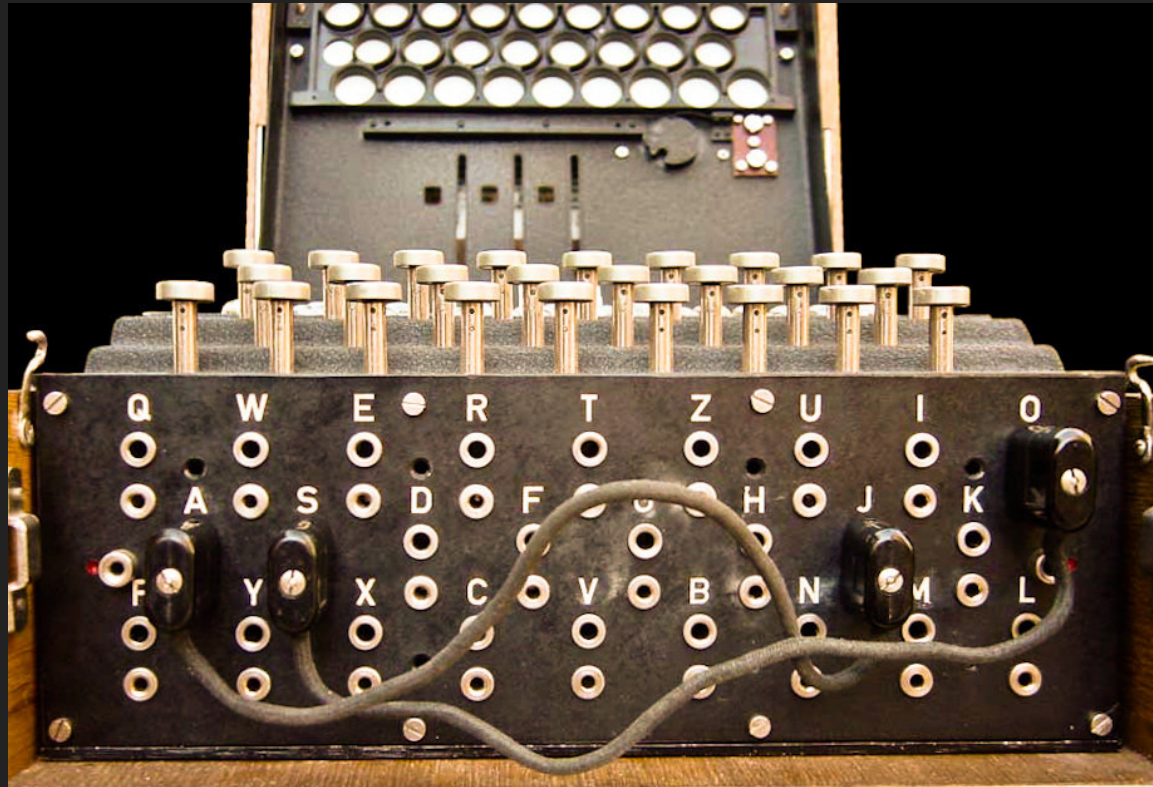
| | | | | | | | |
|-----|---|---|---|---|---|---|---|
| c = | v | o | m | n | w | a | k |
|-----|---|---|---|---|---|---|---|

KERCKHOFF'S PRINCIPLE

"A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."

ENIGMA

(1920)



DES

(1974)

- Key size 2^{56} , block size 64 bits
- Short key sizes can be subject of brute force
- Should be avoided when possible
- Broken in 22 hours
 - See: <https://goo.gl/KgluCi>

DES

(1974)

← → ↻ https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19990119_deschallenge3.html ☆

Electronic Frontier Foundation

FOR IMMEDIATE RELEASE Tuesday, January 19, 1999

RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF)

DES Challenge III Broken in Record 22 Hours

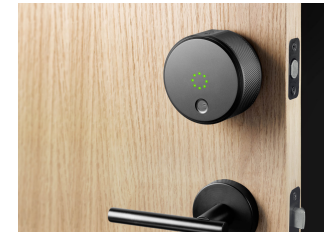
RSA DATA SECURITY CONFERENCE, SAN JOSE, CA -- Breaking the previous record of 56 hours, Distributed.Net, worldwide coalition of computer enthusiasts, worked with the Electronic Frontier Foundation's (EFF) "DES Cra a specially designed supercomputer, and a worldwide network of nearly 100,000 PCs on the Internet, to win RS

A blue classic car, possibly a Ford Mustang, is shown from a rear three-quarter view. The trunk is open, and several large, dark-colored boxes are stacked inside. The car is parked in a dark, industrial-looking environment, possibly a warehouse or garage, with some structural elements visible in the background. The lighting is dramatic, highlighting the car's body and the open trunk.

TODAY

**HARDWARE IS NO
LONGER A
PROBLEM**

DAILY BASIS



BROADER SCOPE

DATA INTEGRITY

SECRECY

SEVERAL PROTOCOLS

AUTHENTICITY

**IT WAS
SUPPOSED TO BE
SIMPLE**

**BUT MOST PART OF
THE TIME IS LIKE**



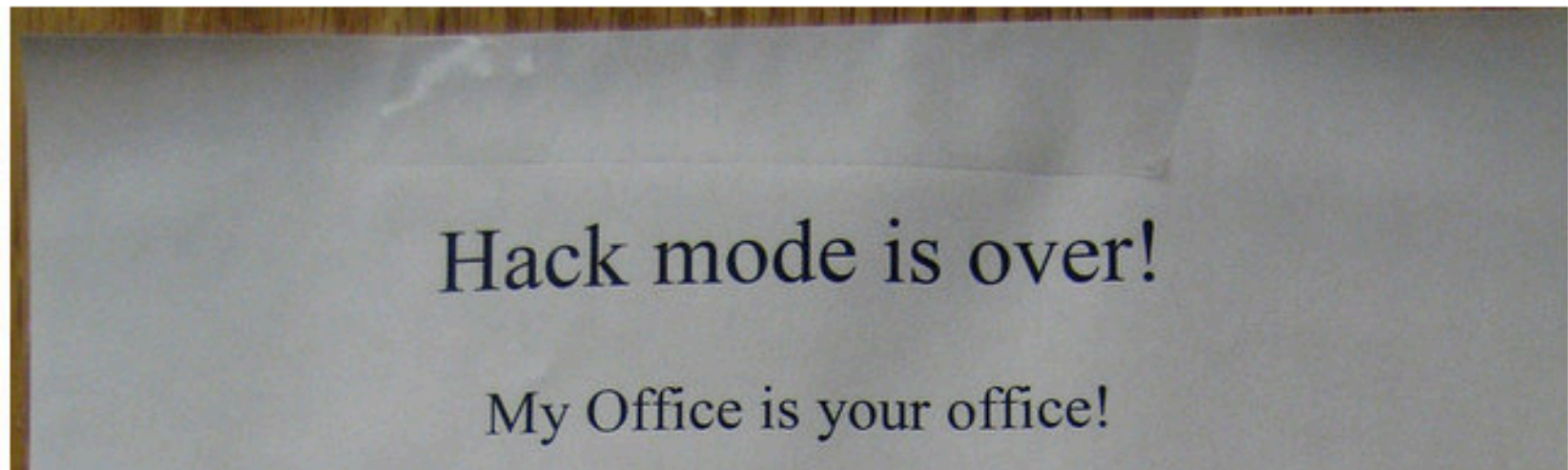
**IT'S REALLY
HARD TO GET IT
RIGHT**


Comodo hacker: I hacked DigiNotar too; other CAs breached

The hacker behind this year's Comodo hack has claimed responsibility for the ...

by **Peter Bright** - Sept 6 2011, 5:36pm EDT

35



 Photograph by **Augie Schwer**

The hack of **Dutch certificate authority DigiNotar** already bore many similarities to the break-in earlier

OCT 20, 2015 @ 12:30 PM 5,923 VIEWS

'No Excuses' As Western Digital Leaves Gaping Crypto Flaws In Hard Drives



Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms.

[FOLLOW ON FORBES \(154\)](#)



FULL BIO ▾

Some serious cryptographers have bloodied foreheads today. They've been facepalming rather vociferously



September 21, 2015

Leaked D-Link security key allows hackers to disguise malware as legit

Share this article:



A leak of a major technology company's security key has been discovered, allowing hackers to convince Windows that their malware is legit.

A company has accidentally released a key that allows hackers to issue malware, disguised as legitimate software.

In February, D-Link, a Taiwanese networking equipment company, published one of its private keys, allowing its software to be recognised as legitimate.

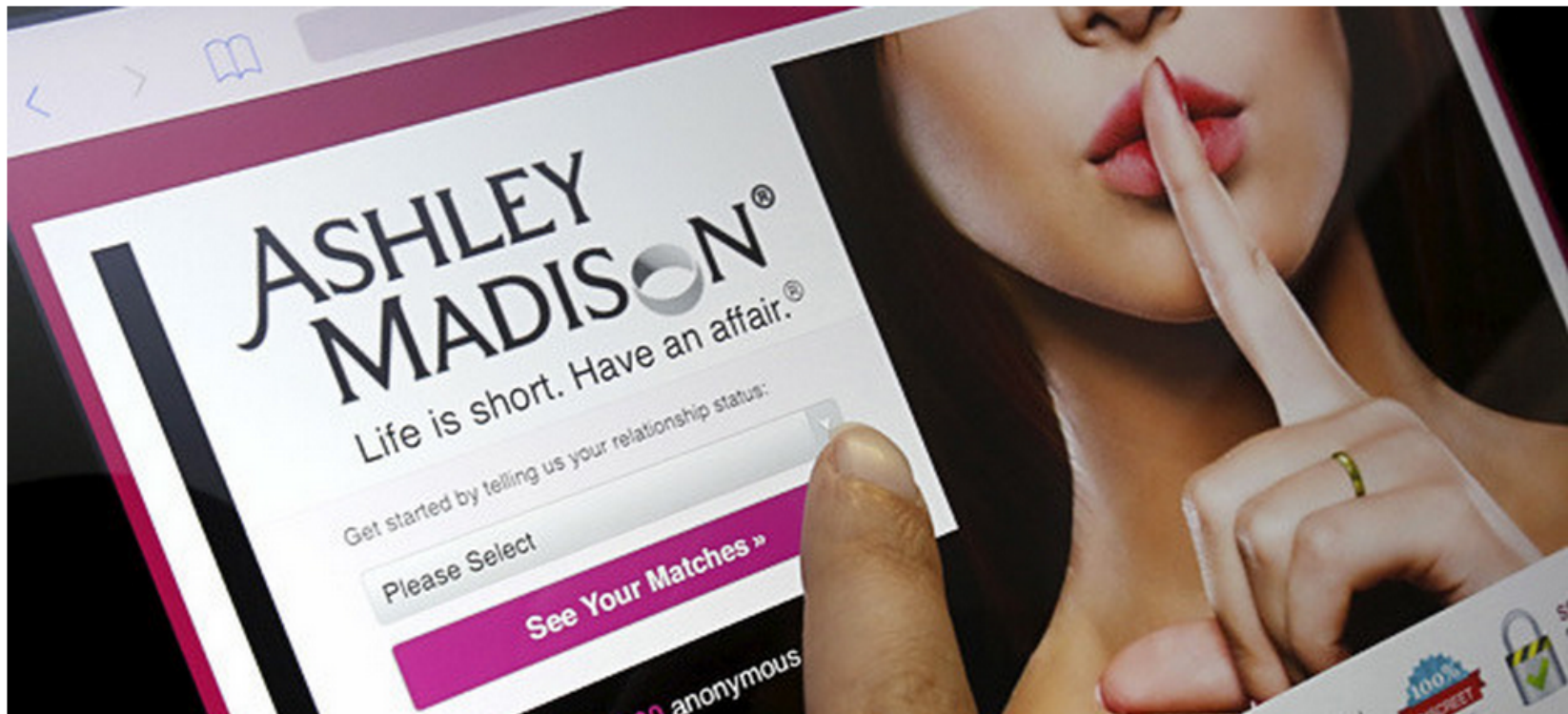
bartvb, a user of Tweakers, a Dutch news outlet, **discovered the leak late last week before reporting it**. The key was discovered when it appeared in one of D-link's open-source firmware downloads for its DCS-5020L surveillance camera.



The leaked key has been published since february of this year

ASHLEY MADISON BREACH

Ashley Madison hackers publish compromised records



HEARTBLEED



SURVEILLANCE





"Security is the Jar Jar Binks of software development."


Martin Boßlet

A photograph of a dirt path in a forest that splits into two directions. The path is covered in fallen leaves and leads into a dense forest of tall trees with green foliage. The scene is slightly blurred, giving it a dreamlike or contemplative feel. A dark rectangular box is superimposed over the center of the image, containing the text "PROBLEM OR SOLUTION?".

**PROBLEM OR
SOLUTION?**

| Vulnerability | Financial Services | Government | Healthcare | Manufacturing | Retail & Hospitality | Technology | Other | Rank |
|----------------------------|--------------------|------------|------------|---------------|----------------------|------------|-------|------|
| Code Quality | 65% | 70% | 80% | 56% | 68% | 70% | 65% | 1 |
| Cryptographic Issues | 60% | 66% | 61% | 51% | 63% | 62% | 59% | 2 |
| Information Leakage | 58% | 62% | 60% | 49% | 55% | 62% | 53% | 3 |
| CRLF Injection | 52% | 52% | 48% | 45% | 54% | 54% | 48% | 4 |
| Cross-Site Scripting (XSS) | 49% | 51% | 46% | 45% | 52% | 49% | 47% | 5 |
| Directory Traversal | 48% | 48% | 45% | 40% | 44% | 48% | 46% | 6 |

Source: Veracode



**BOOKS
ARE AN AMAZING
SOURCE TO LEARN**

Why shouldn't we roll our own?



81

Why shouldn't we create our own security schemes?

I see a lot of questions around here about custom crypto and custom security mechanisms, especially around password hashing.



With that in mind, I'm looking for a canonical answer, with the following properties:



33

- Easy for a newbie to understand.
- Clear and explicit in *why* rolling your own is a bad idea.
- Provides strong examples.

[Obligatory xkcd.](#)

Source: Stackoverflow

**DON'T ROLL
YOUR OWN
CRYPTO**

CAVP: Cryptographic Algorithm Validation Program

CAVP Testing Specifications

Symmetric Key:
-AES, TDES

Additional Modes of Operation:
-XTS-AES

Asymmetric Key:
-DSA, ECDSA, RSA (FIPS 186-2 / FIPS 186-4)

SHS

RNG

DRBG

Key Management:
-Key Agreement Schemes (KAS) and Key Confirmation Algorithms

MAC:
-CMAC, CCM, GCM/GMAC,

[CSRC HOME](#) > [GROUPS](#) > [STM](#) > [CAVP](#)

CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM (CAVP)

The ***Cryptographic Algorithm Validation Program (CAVP)*** encompasses validation testing for FIPS approved and NIST recommended cryptographic algorithms and components of algorithms. Cryptographic algorithm validation is a prerequisite to the Cryptographic Module Validation Program (CMVP). The CAVP was established by NIST and the Communications Security Establishment (CSE) in July 1995. All of the tests under the CAVP are handled by third-party laboratories that are accredited as Cryptographic and Security Testing (CST) Laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). Vendors interested in validation testing of their algorithm implementation may select any of the accredited laboratories.

CRYPTOGRAPHIC ALGORITHM VALIDATION TESTING SPECIFICATIONS

Below are the algorithms for which the CAVP currently



HOW CRYPTO IS DONE NOWADAYS?

The image is a composite graphic. The background is a photograph of a large concrete dam and a reservoir, with steep, rocky mountains in the distance. The sky is overcast. Overlaid on the right side of the image are several geometric elements: a diagonal band of a repeating hexagonal pattern, and several solid-colored diagonal bands in shades of orange and yellow. A dark, semi-transparent horizontal banner spans the middle of the image, containing the text "FULL CONTROL" in a bold, white, sans-serif font.

FULL CONTROL



GOOD

BAD



LET'S GET OUR
HANDS DIRTY

THE BADLY DESIGNED NOTE APP

TOOLS

Java 8

org.json

BouncyCastle

Hmmm, I wish I had a
journal app to share my
notes



ALICE

Yes, we can!

BOB



Must be nice!

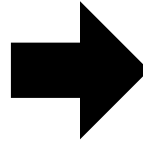


EVE

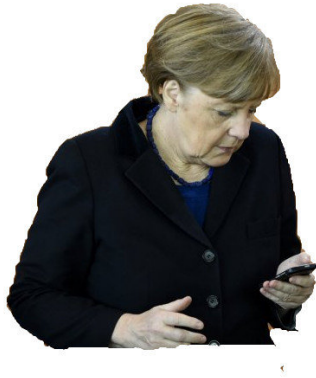
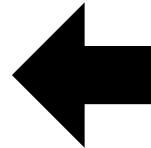
#1 STORY

**AS A USER OF THIS
APP, ALICE WANTS
TO BE ABLE TO
CREATE NEW
ENTRIES**

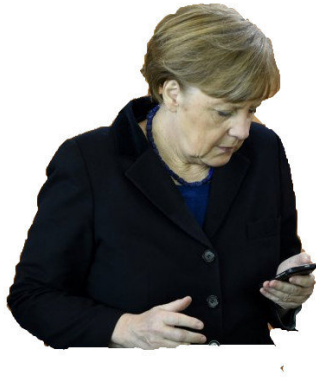
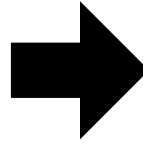
WHASSSSSSSUP?



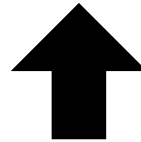
WHASSSSSSSUP?



WHASSSSSSSUP?



You can't process me
with a normal brain.



#2 STORY

**AS A USER OF THIS
APP, BOB WANTS TO
BE ABLE TO VERIFY
THE INTEGRITY OF
ALICE'S FILES**

CWE-327

**USE OF A BROKEN OR
RISKY
CRYPTOGRAPHIC
ALGORITHM**

MD5

ARE THEY DIFFERENT?



SHA-1

<https://malicioussha1.github.io/>

**BUT WHAT ABOUT
INCLUDING A SALT?**

CWE-916
PASSWORD HASH
WITH
INSUFFICIENT
COMPUTATIONAL
EFFORT

SHA-224

SHA-256

SHA-384

SHA-512

ARE ALL GOOD CHOICES

HowToSHA256SUM

The program **sha256sum** is designed to verify data integrity using the SHA-256 (SHA-2 family with a digest length of 256 bits). SHA-256 hashes used properly can confirm both file integrity and authenticity. SHA-256 serves a similar purpose to a prior algorithm recommended by Ubuntu, **MD5**, but is less vulnerable to attack.

Comparing hashes makes it possible to detect changes in files that would cause errors. The possibility of changes (errors) is proportional to the size of the file; the possibility of errors increase as the file becomes larger. It is a very good idea to run an SHA-256 hash comparison check when you have a file like an operating system install CD that has to be 100% correct.

In terms of security, cryptographic hashes such as SHA-256 allow for authentication of data obtained from insecure mirrors. The SHA-256 hash must be signed or come from a secure source (such as a HTTPS page or a GPG-signed file) of an organization you trust. See the SHA256 file for the release you're using under <http://releases.ubuntu.com>, such as <http://cdimage.ubuntu.com/daily-live/current/SHA256SUMS>. You should verify this file using the **PGP** signature, SHA256SUMS.gpg (such as <http://cdimage.ubuntu.com/daily-live/current/SHA256SUMS.gpg>). You could avoid the signature verification step if you relied on SHA-256 hashes learned from **UbuntuHashes** (a secure unmodifiable page). However, as of December 2009 this page does not include such hashes.

Contents

1. [sha256](#)
2. [sha256sum on Linux](#)
 1. [Check the iso file](#)
 2. [Check the CD](#)
3. [digest\(1\) on Solaris](#)
4. [SHA256SUM of burnt media](#)
5. [External Links](#)

sha256

sha256sum on Linux

#3 STORY

**AS A PARANOID, I
WOULD LIKE NOT
ONLY INTEGRITY,
BUT ALSO
AUTHENTICITY**

#4 STORY

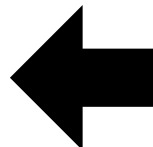
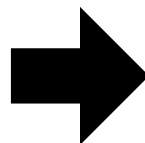
**AS A USER OF THIS APP, I
WANT TO ADD
INTEGRITY,
AUTHENTICITY AND
SECRECY AND HIDE MY
ENTRIES FROM NSA**

PADDING

**WE USE A "PADDING
SCHEME" TO FILL THE
LAST BLOCK
UNTIL IT MEETS THE
CIPHER BLOCK SIZE**



Key

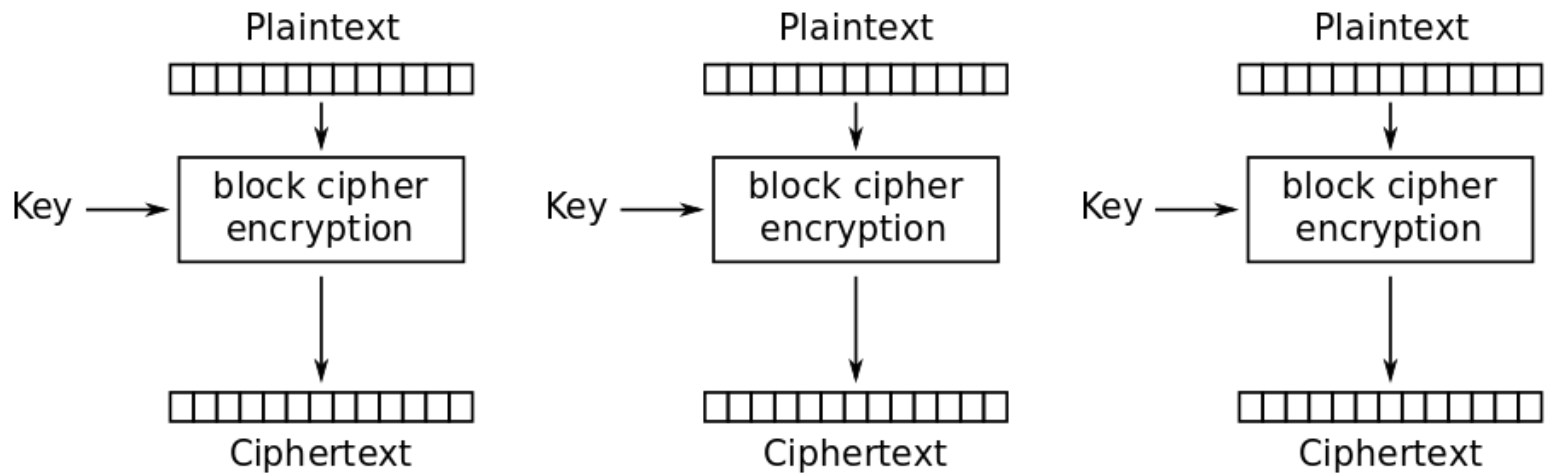


Key



The background image shows a massive concrete dam situated in a deep, rocky gorge. The sky above is dark and cloudy, while the foreground shows the calm water of the reservoir. A prominent yellow geometric pattern, consisting of a series of interconnected hexagons, runs diagonally across the right side of the image. The title text is centered within a dark, semi-transparent rectangular box.

MODES OF OPERATION

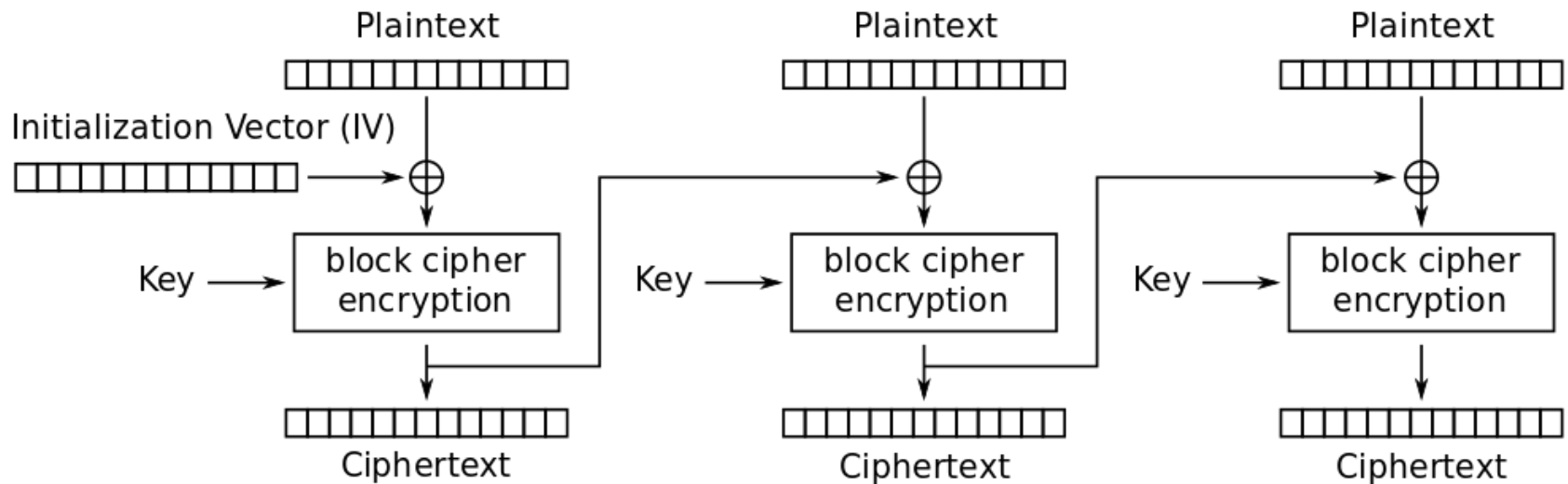


Electronic Codebook (ECB) mode encryption

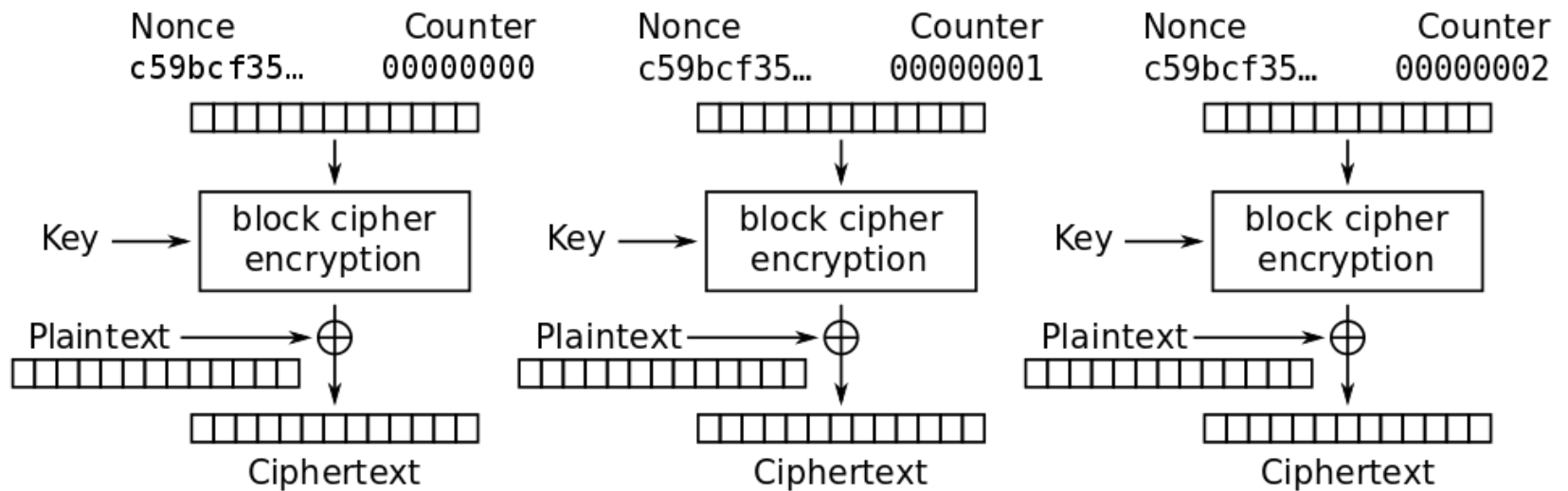
Source: Wikipedia



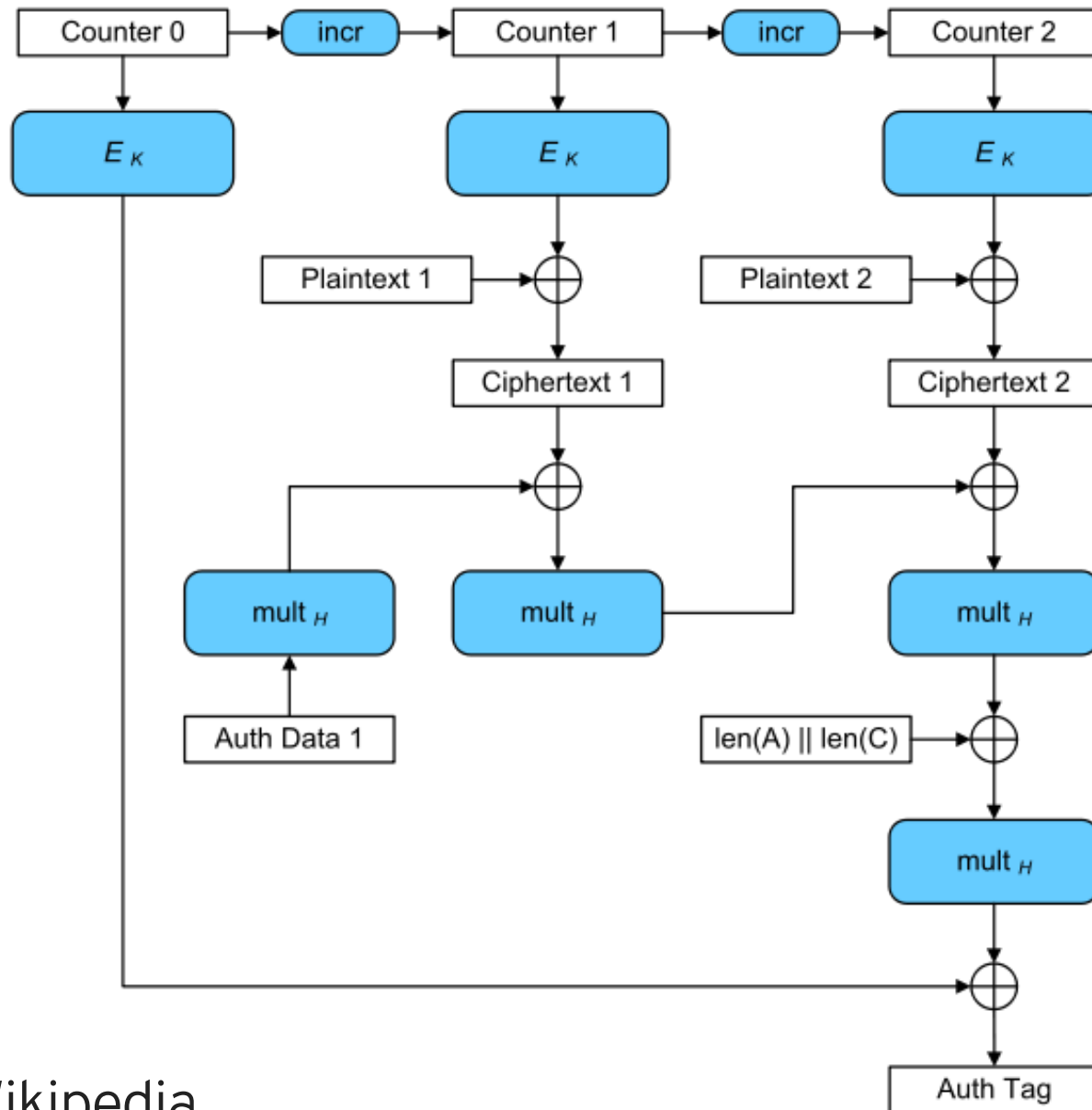
**Everybody knows ECB
mode is bad because
we can see the penguin**



Cipher Block Chaining (CBC) mode encryption



Counter (CTR) mode encryption



Source: Wikipedia

#5 STORY

**AS A USER I WANT TO
HAVE PASSWORD
PROTECTED ENTRIES**

#6 STORY

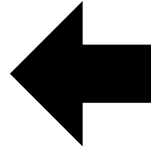
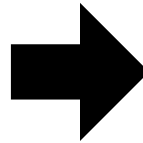
**AS SOMEONE VERY
SOCIAL, I WANT TO
SHARE MY ENTRIES WITH
A FRIEND WITHOUT
EXPOSING MY KEYS**



sK



pK



sK



pK





redhat.®

**THANK
YOU!**

<http://abstractj.org>

<https://aerogear.org>