

# ¿Que dice aca?

Tm9zLCBsb3MgcmVwcmVzZW50YW50ZXMGZGVsIHB1ZWJsbyBkZSBsYSBOYWNP824g  
QXJnZW50aW5hLCByZXVuaWRvcyBlbiBDb25ncmVzbyBHZW5lcmFsIENvbnN0aXRl  
eWVudGUgcG9yIHZvbHVudGFkIHkgZWxlY2Np824gZGUgbGFzIHByb3ZpbmNpYXMg  
cXVlIGxhIGNvbXBvbmVulCBlbjBjdWlwbGltaWVudG8gZGUgcGFjdG9zIHByZWV4  
aXN0ZW50ZXMsIGNvbiBlbCBvYmpldG8gZGUgY29uc3RpdHVpciBsYSBlbmNzbiBu  
YWNpb25hbCwgYWZpYW56YXIgbGEganVzdGljaWEsIGNvbnNvbGlkYXIgbGEgcGF6  
IGludGVyaW9yLCBwcm92ZWVyIGEgbGEgZGVmZW5zYSBjb236biwgCHJvbW92ZXI  
gZWwgYmllbmVzdGFyIGdlbmVyYWwsIHkgYXNlZ3VyYXIgbG9zIGJlbmVmaWNpb3Mg  
ZGUgbGEgbGllZXJ0YWQgcGFyYSBub3NvdHJvcywgcGFyYSBudWVzdHJhIHBvc3Rl  
cmllkYWQgeSBwYXJhIHRvZG9zIGxvcyBob21icmVzIGRlbCBtdW5kbyBxdWUgcXVp  
ZXJhbiBoYWJpdGFyIGVuIGVsIHN1ZWxvIGFyZ2VudGlubzsgaW52b2NhbmRvIGxh  
IHByb3RlY2Np824gZGUgRGlvcywgZnVlbnRlIGRlIHRvZGEgcGF6824geSBqdXN0  
aWNpYTogb3JkZW5hbW9zLCBkZW50ZXRhbm9zIHkgZXN0YWJsZW50bW9zIGVzdGEg  
Q29uc3RpdHVjaFNUIHBhcmEgbGEgTmFjaFNUIEFyZ2VudGluYS4gCg==

- **Mecanismo de codificación que utiliza un conjunto de 64 caracteres para codificar cualquier valor posible de un byte. Toma 3 bytes, y los convierte en 4. Usa A-Z,a-z,0-9,+,/ e = para el padding**

Ej: **“Mensaje en claro”**

Codificado en base 64:

**TWVuc2FqZSBIbiBjbGFybwo=**

- **Multipurpose Internet Mail Extensions (MIME) es un estándar de internet (rfc 2045 y sigs.) que extiende el formato de los emails para soporta texto en sets de caracteres distintos al US-ASCII, binarios anexados, mensajes que incluyan distintos tipos de objetos. Los tipos de contenidos definidos por MIME son muy utilizados en otros protocolos como por ejemplo HTTP.**

# Ejemplos de Content-type

- text
  - text/plain
  - text/richtext
- message
  - message/rfc822
- image
  - image/jpeg
  - image/gif
- video
  - video/mpeg
- application
  - application/PostScript
  - application/octet-stream
- multipart
  - multipart/mixed
  - multipart/alternative

- **S/MIME (Secure / Multipurpose Internet Mail Extensions) es un estándar para cifrado de clave pública y firma de emails. Define el content-type application/pkcs7...**
- **La funcionalidad de S/MIME está implementada en la mayoría de los clientes de correo electrónico.**

# Servicios Provistos por S/MIME

- **Autoria**
- **Integridad del mensaje**
- **No repudio**
- **Confidencialidad de los datos**



**Implementación Open Source de diversos algoritmos y estándares criptográficos. <http://www.openssl.org>**

**Documentación de uso:**

**<http://www.madboa.com/geek/openssl/>**

- Definición: Es un tipo de ataque basado en información obtenida (de un efecto secundario) de la implementación del algoritmo criptográfico y no basada en debilidades del algoritmo en sí.
- Tipos de Side Channels:
  - Tiempo: basados en cuánto tardan ciertos cálculos.
  - Consumo eléctrico: basados en diferencias de consumo del hardware dependiendo de la operación realizada.
  - Electromagnéticos: basados en información fugada como radiación electromagnética.
  - Acústico: basados en sonidos emitidos durante el cómputo.
  - etc.



- **Dependiendo de como se genera e intercambia la clave de sesión, en, por ejemplo, ssl, el que obtenga la clave privada del servidor, podría descifrar todas las comunicaciones previas.**
- **Para evitar eso se usa Forward Secrecy.**

**Ref: <https://community.qualys.com/blogs/securitylabs/2013/06/25/ssl-labs-deploying-forward-secrecy>**

# Padding Oracle Attacks

- Escenario: Una aplicación que utiliza un cifrador de bloques en modo CBC y padding PKCS#5. La aplicación responde de la siguiente manera:
  - Texto valido correctamente cifrado: respuesta normal.
  - Texto inválido correctamente cifrado: error indicando que el valor recibido no es válido.
  - Texto con cifrado incorrecto (padding incorrecto): error indicando falla de padding.
- En este escenario el ataque nos permite descifrar el mensaje y cifrar un mensaje arbitrario (sin conocer la clave simétrica).
- Ref: <http://netifera.com/research/poet/PaddingOracleBHEU10.pdf>

- **Mental Poker**
- **Zero-knowledge proofs**  
<https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/>
- **Smart Contracts**
- **Homomorphic Encryption and secret sharing**
- **Digital Cash**

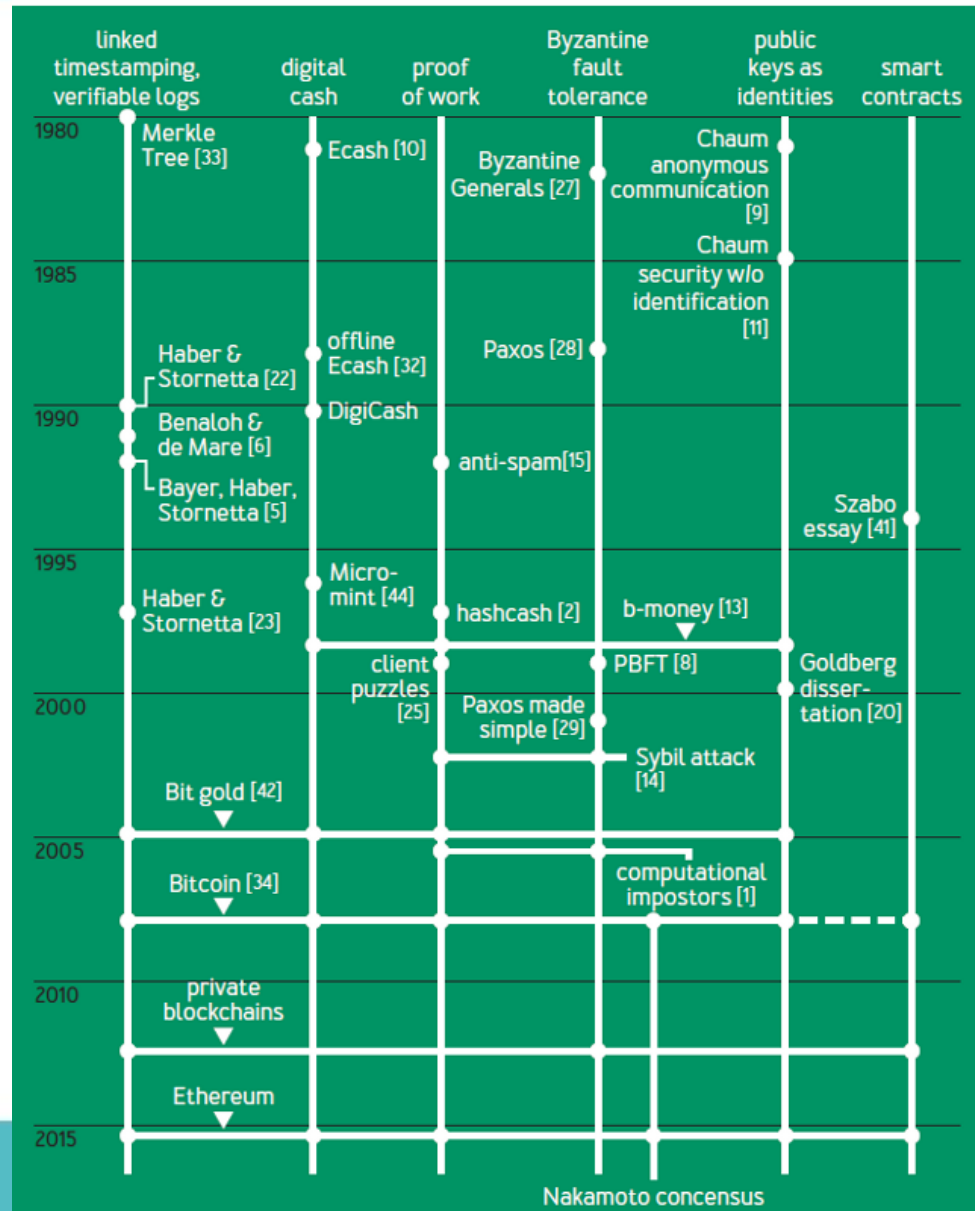
- **Es un tema muy grande.**
- **Un curso interesante:**

**<https://piazza.com/princeton/spring2015/btctech/home>**

# Bitcoin's Academic Pedigree



FIGURE 1: CHRONOLOGY OF KEY IDEAS FOUND IN BITCOIN



<http://queue.acm.org/detail.cfm?id=3136559>

# Más bibliografía

