

Marca de tiempo confiable

IEEE capítulo computación
Juan Pechiar



Nada nuevo...



El presente correo y cualquier posible archivo adjunto está dirigido únicamente al destinatario del mensaje y contiene información que puede ser confidencial. Si Ud. no es el destinatario correcto por favor notifique al remitente respondiendo anexando este mensaje y elimine inmediatamente el e-mail y los posibles archivos adjuntos al mismo de su sistema. Está prohibida cualquier utilización, difusión o copia de este e-mail por cualquier persona o entidad que no sean las específicas destinatarias del mensaje. XXXXX no acepta ninguna responsabilidad con respecto a cualquier comunicación que haya sido emitida incumpliendo nuestra Política de Seguridad de la Información

Tercero de confianza



Wednesday, 17 August 2011

Funciones de hash



Wednesday, 17 August 2011

CONTRATO

Este es un
contrato por
UYU 1000

función de hash



F3 D7 90

CONTRATO

Este es un
contrato por
UYU 2000



37 4B 51

Muy difícil fabricar un
documento con el
mismo hash que otro

El hash representa al
documento pero no
contiene información del
mismo

La clave

La clave
tiene 2 partes

La parte “privada” no
se muestra a nadie

La parte “pública” se
publica

CERTIFICADO

La parte pública de
la clave de JUAN es
152652198734

firma: La Autoridá

CERTIFICADO

La parte pública de
la clave de La
Autoridá es
57197592983741

firma: La Autoridá

Encripto con $K_{\text{púb_juan}}$

Sólo desencrypto con
 $K_{\text{priv_juan}}$

Encripto con $K_{\text{priv_juan}}$

Sólo desencrypto con
 $K_{\text{púb_juan}}$

Encriptado

Firma

Marca de tiempo

hash del documento

+

fecha y hora

+

firma digital de TSA

Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

RFC 3161

ANSI ASC X9.95



ISO/IEC 18014

Ejemplo: Registro de propiedad intelectual

Nov. 18, 1941.

F. E. WOLCOTT

2,262,982

TOOTHBRUSH

Filed Aug. 24, 1938

Fig. 1.

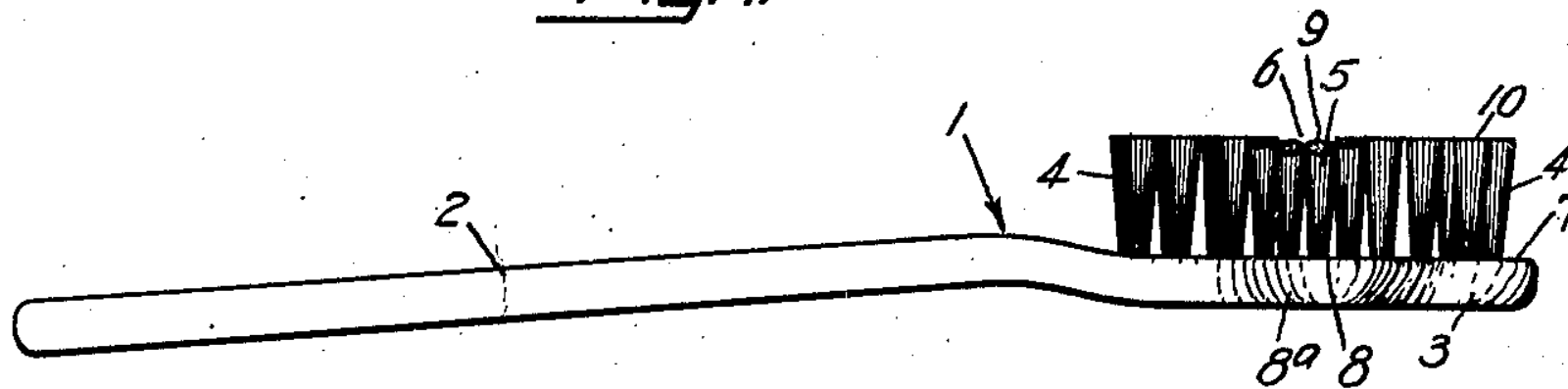


Fig. 2.

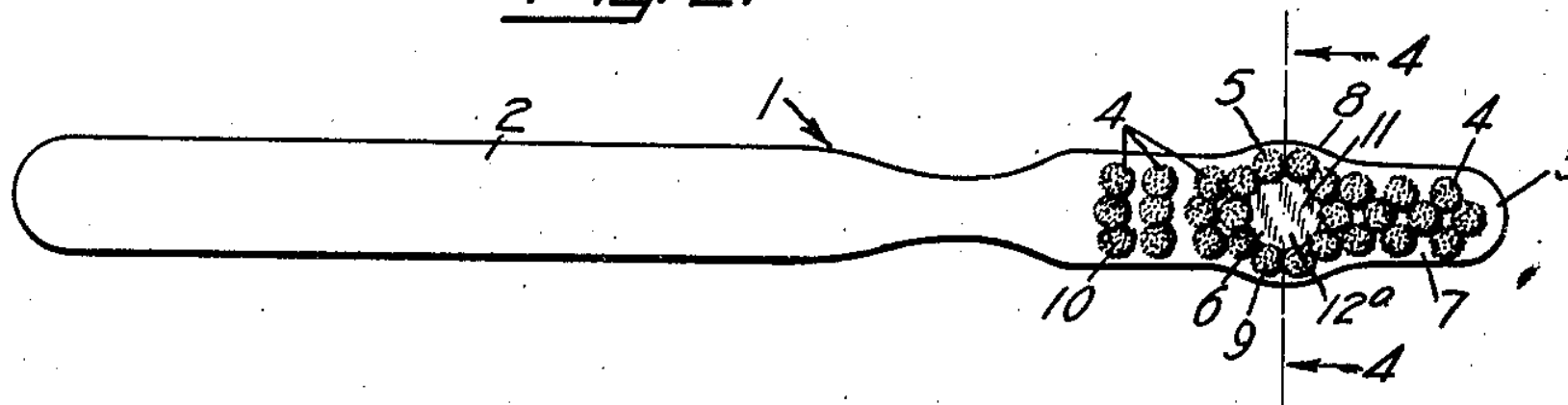


Fig. 3.



Fig. 4.

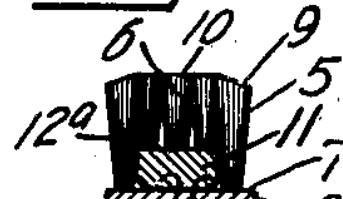
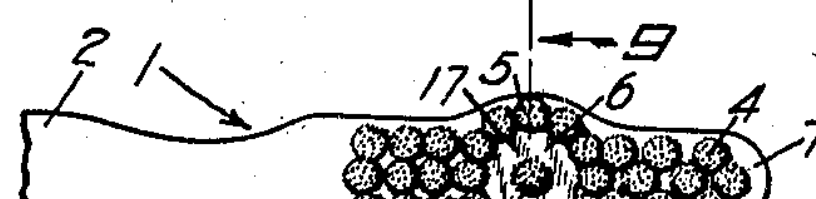


Fig. 7.





Wednesday, 17 August 2011

Ejemplo: Registro de documentos notariales

ion NO convalida los actos y negocios jurídicos nulos y
ni subsana los vicios o defectos de que adolecieren
las leyes (art. 62 Ley 16871)

FIRMA DEL REGISTRADOR

MINISTERIO DE EDUCACION Y CULTURA

DIRECCION GENERAL
DE REGISTROS

REPUBLICA ORIENTAL DEL URUGUAY

Ejemplo: Cierre de llamados / licitaciones





¿Qué hora es?



