

Infraestructuras de claves publicas

Fernando Virdia

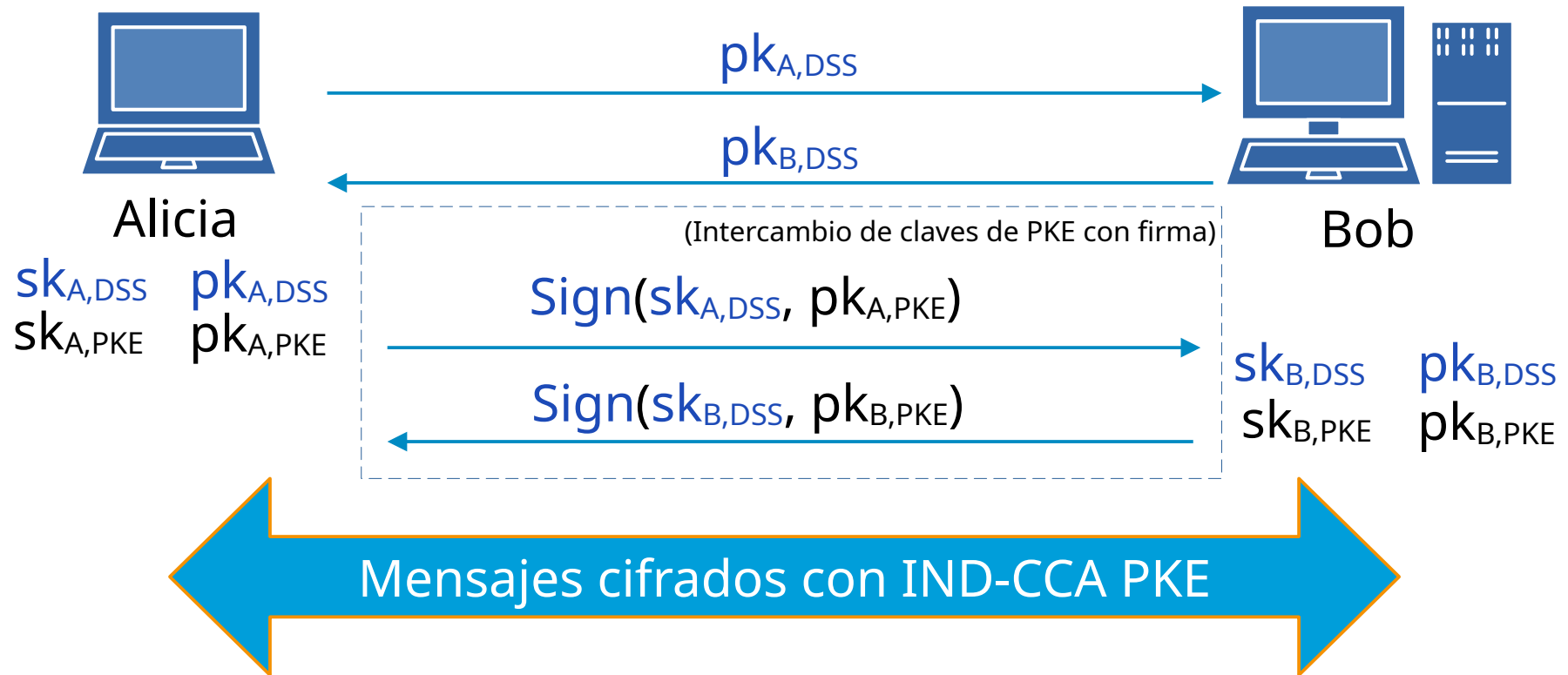
<https://apuntes.indcpa.com>

Versión 0.1, junio 2025

Resumen de la situación

- Juntando cifrados simétricos autenticados (AE) y un KEM, logramos obtener cifrado de clave pública (PKE) resistente a ataques de un adversario “activo”
- También logramos construir sistemas de firma digital (DSS)
- Ahora necesitamos autenticar el intercambio de claves públicas de PKE entre partes que no se conocen
- Para eso exploramos varias opciones para una infraestructura de claves públicas (PKI, “*public key infrastructure*”)

Intento #1



Intento #1



Alicia

$sk_{A,DSS}$ $pk_{A,DSS}$
 $sk_{A,PKE}$ $pk_{A,PKE}$

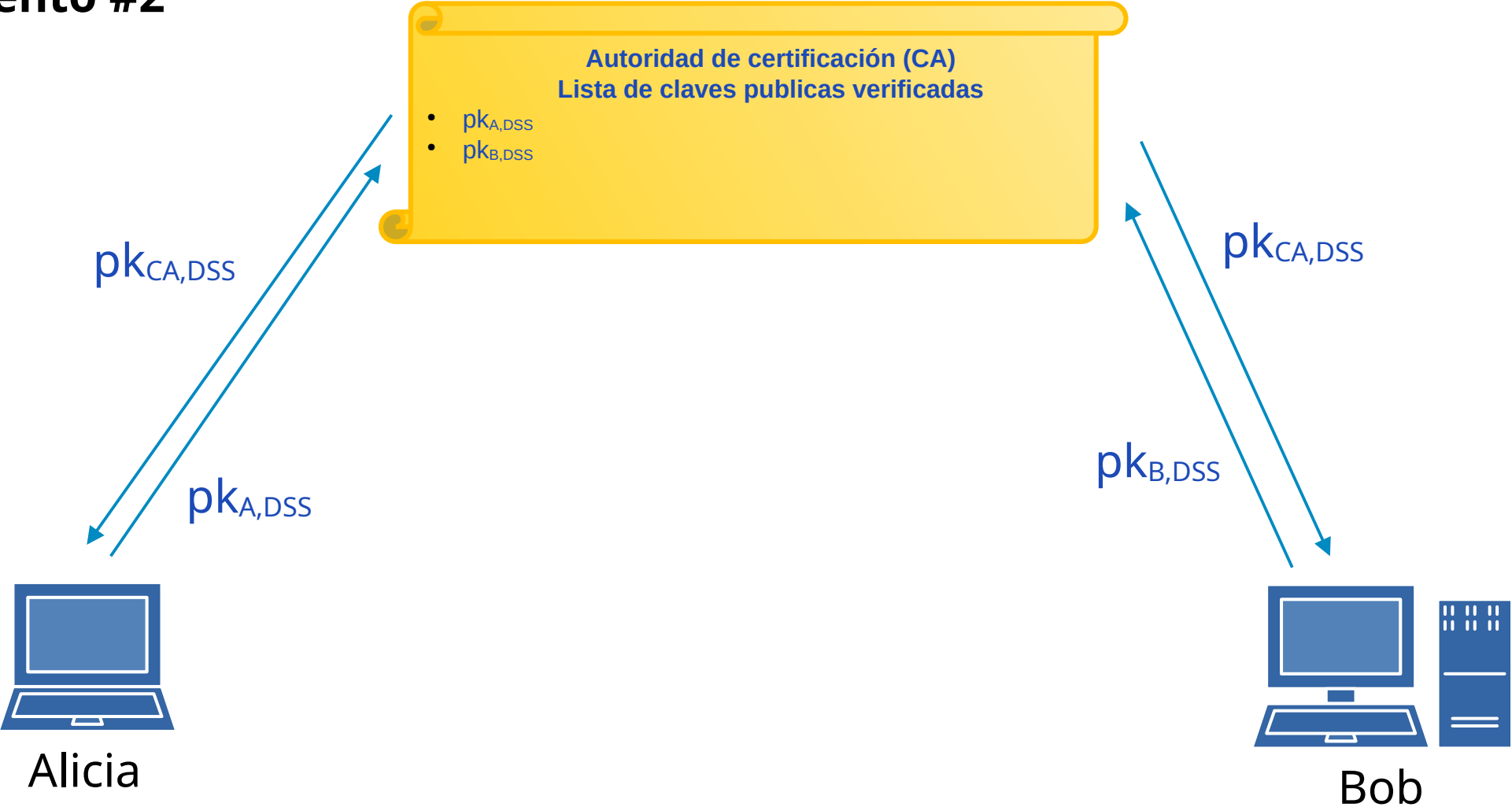
- Este es parecido al sistema de los “*key signing parties*” donde individuos se encuentran de persona para firmar claves publicas de conocidos
- Requiere encontrarse con la persona con la cual queremos comunicar...
- O confiar en conocidos en común
- Sin confianza no hay autenticación



Bob

$sk_{B,DSS}$ $pk_{B,DSS}$
 $sk_{B,PKE}$ $pk_{B,PKE}$

Intento #2



Intento #2

Autoridad de certificación (CA) Lista de claves publicas verificadas

- $pk_{A,DSS}$
- $pk_{B,DSS}$

- La autoridad es publica, el intercambio podría autenticarse de persona
 - Una sola autoridad es inconveniente...
- El CA genera un certificado por cada clave



Alicia
 $pk_{CA,DSS}$

Cert CA $\rightarrow$ A

- $pk_{A,DSS}$
- $\text{Sign}(sk_{CA,DSS}, "pk_{A,DSS}$
le pertenece a A y
vale desde xx/yy
hasta ww/zz")

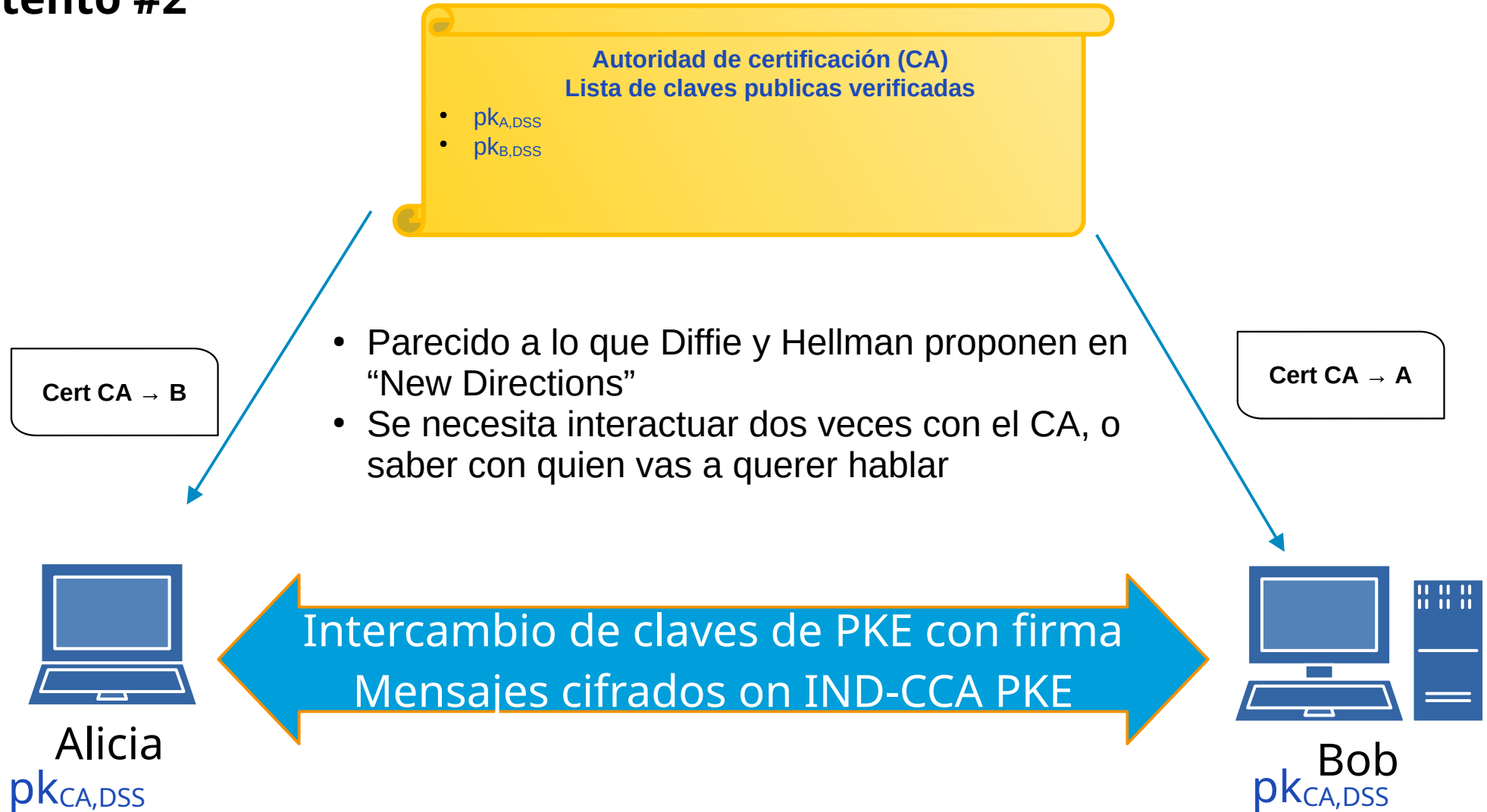
Cert CA $\rightarrow$ B

- $pk_{B,DSS}$
- $\text{Sign}(sk_{CA,DSS}, "pk_{B,DSS}$
le pertenece a B y
vale desde xx/yy
hasta ww/zz")



Bob
 $pk_{CA,DSS}$

Intento #2



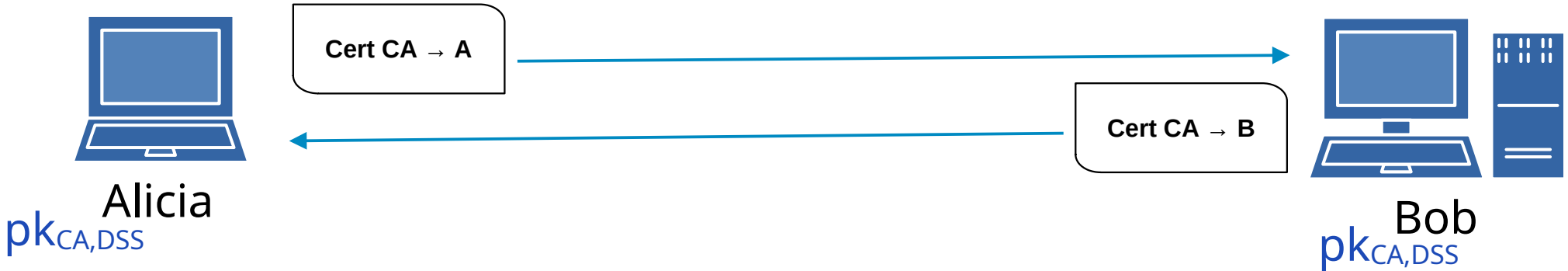
Intento #3



Intento #3

Autoridad de certificación (CA)
Lista de claves publicas verificadas

- $pk_{A,DSS}$
- $pk_{B,DSS}$



Intento #3

Autoridad de certificación (CA)
Lista de claves publicas verificadas

- $pk_{A,DSS}$
- $pk_{B,DSS}$



Alicia



Intercambio de claves de PKE con firma
Mensajes cifrados on IND-CCA PKE



Bob

Intento #3

Autoridad de certificación (CA)
Lista de claves publicas verificadas

- $pk_{A,DSS}$
- $pk_{B,DSS}$

- Aun una sola autoridad, con la cual es necesario una interacción “autenticada”
- Ambas partes necesitan un certificado
 - En la practica es común que Alicia no presente certificado, y Bob suponga de interactuar con una parte anónima (podría usar un sistema de login para autenticar Alicia)

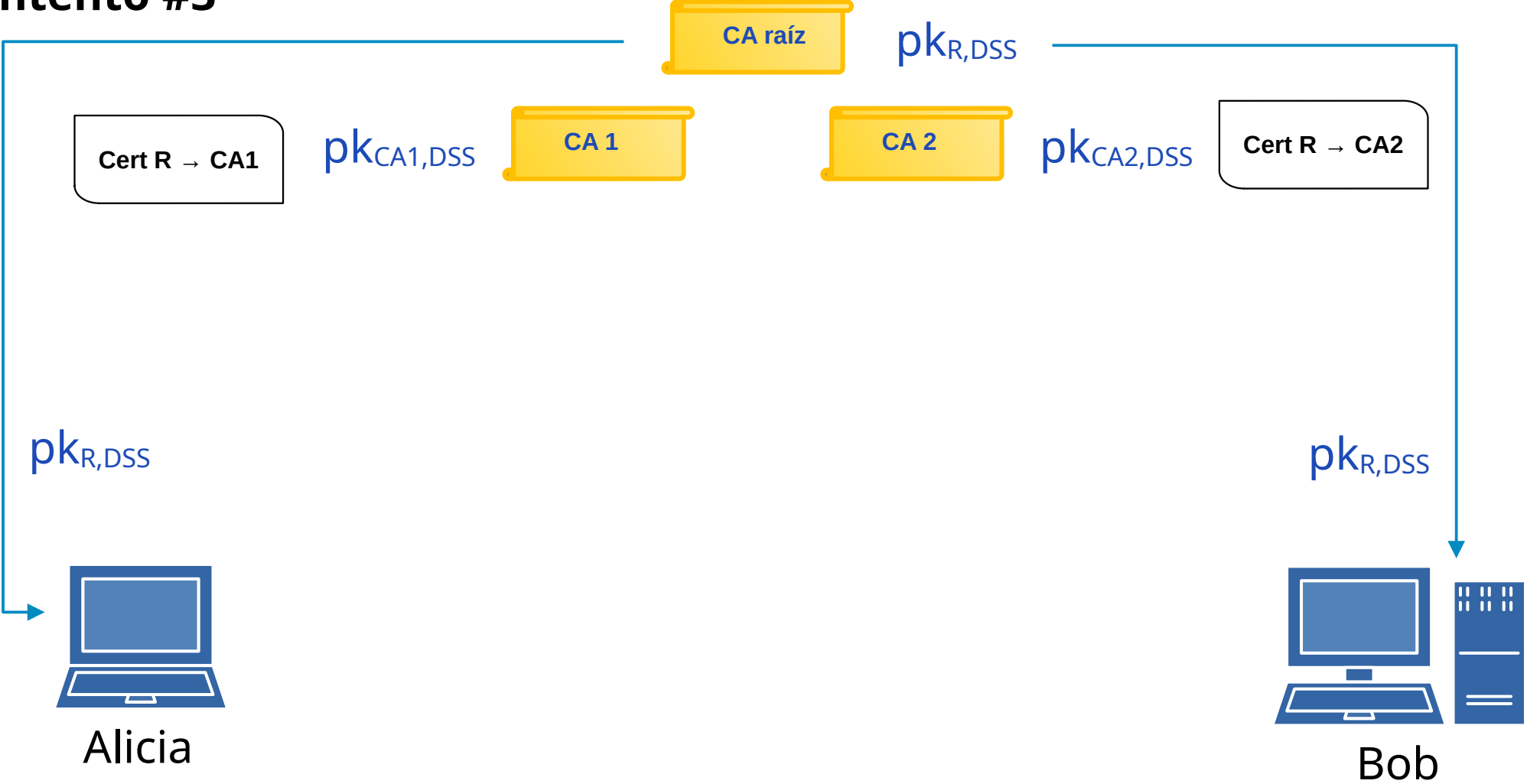


Alicia

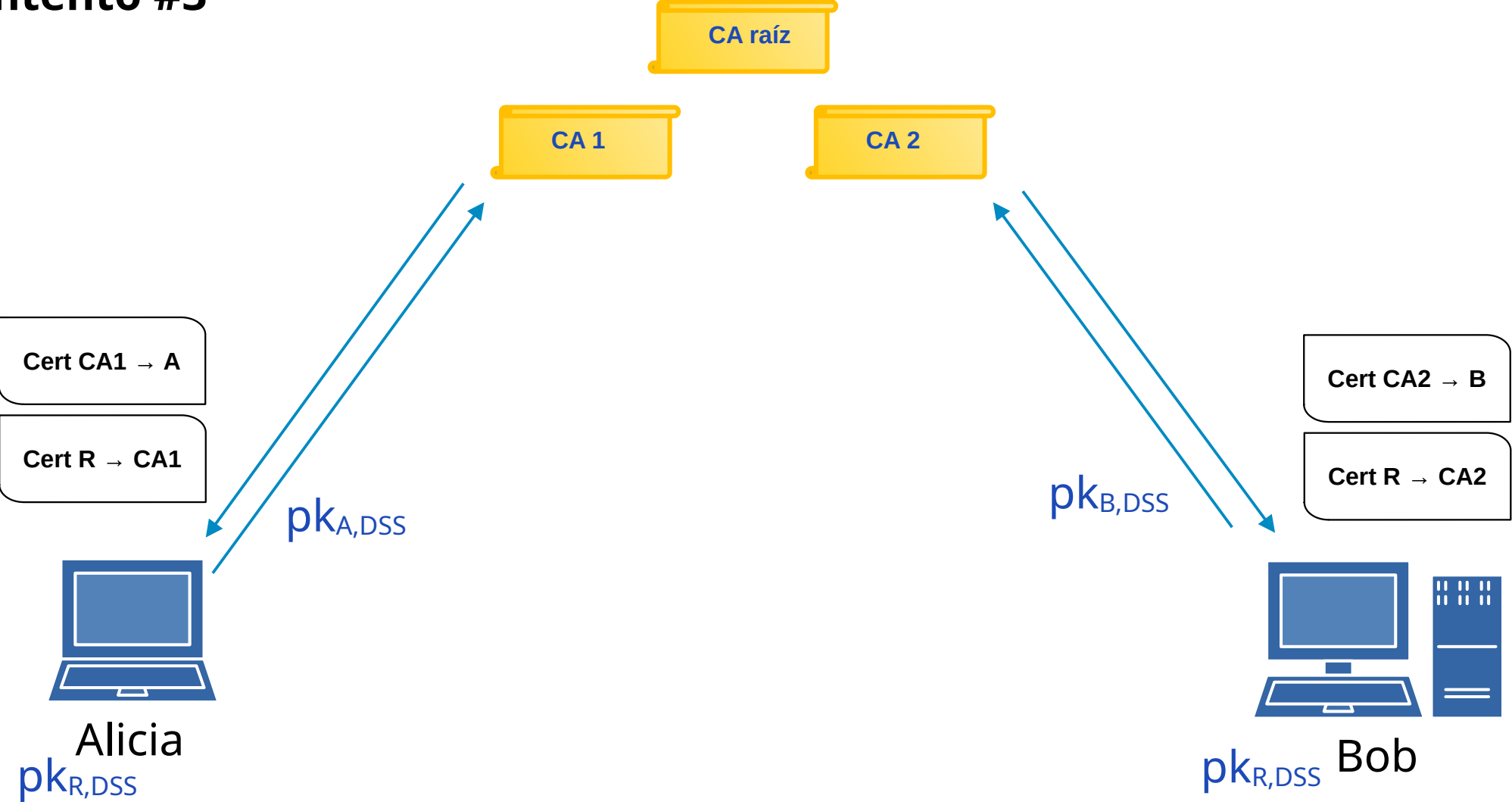


Bob

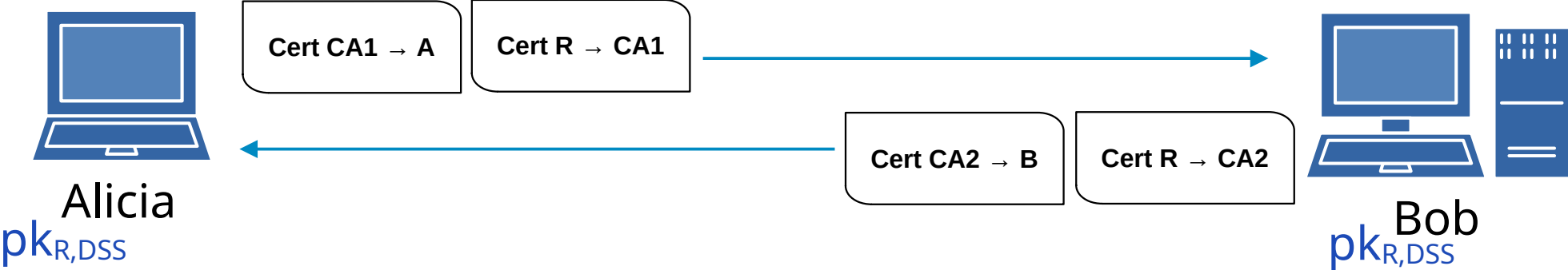
Intento #3



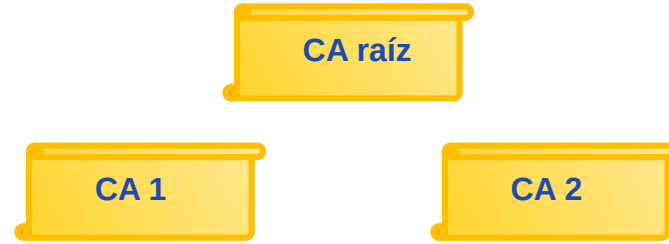
Intento #3



Intento #3



Intento #3



Alicia



Bob

Intento #3



- Mas de una autoridad, posiblemente sea mas fácil autenticarse para Alicia y Bob si se encuentran en diferentes contextos
- Ahora hay que confiar en mas de un CA!
 - En el que uno usa para su propio certificado
 - Y en el que las otras partes usan, también

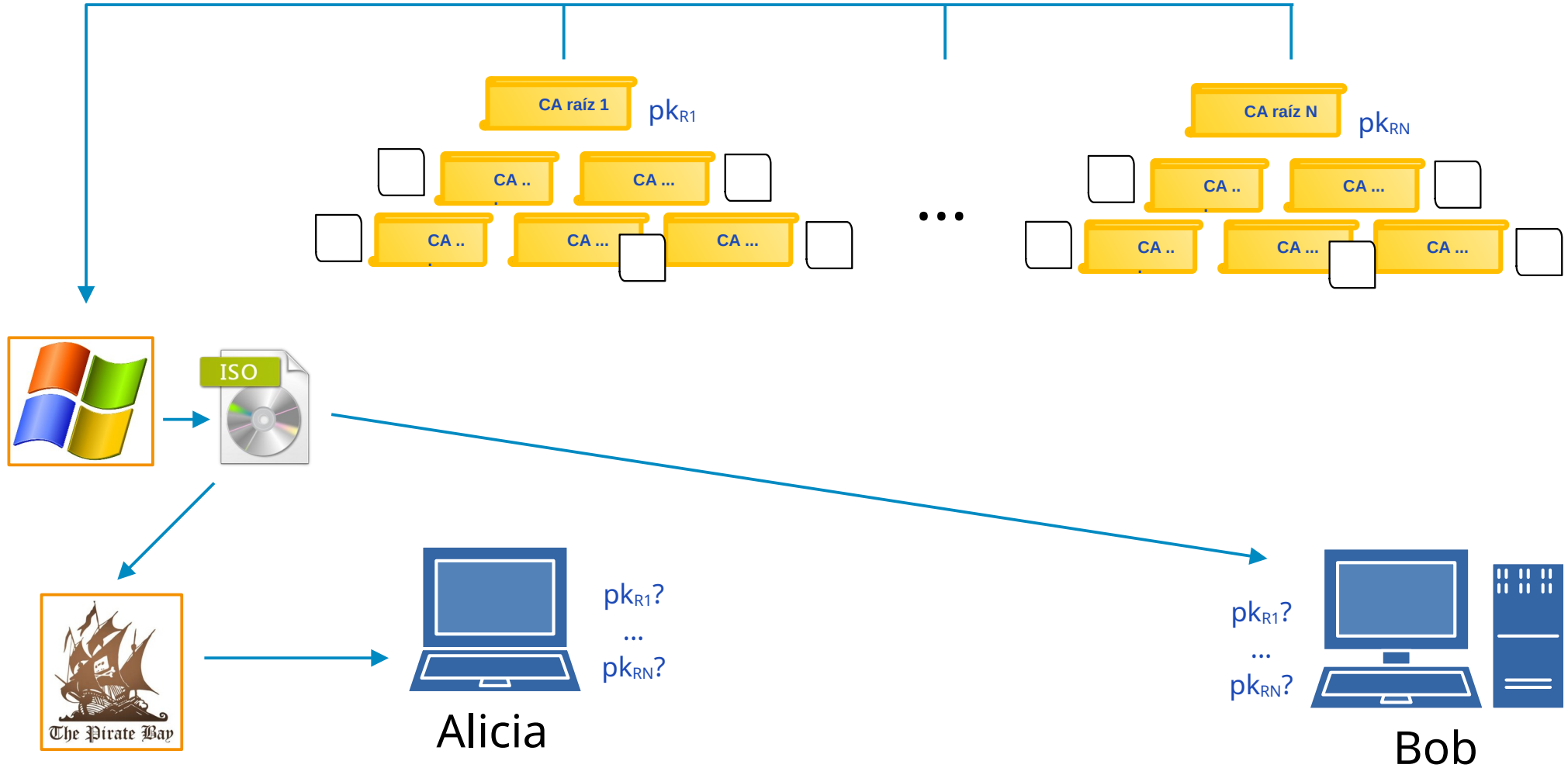


Alicia

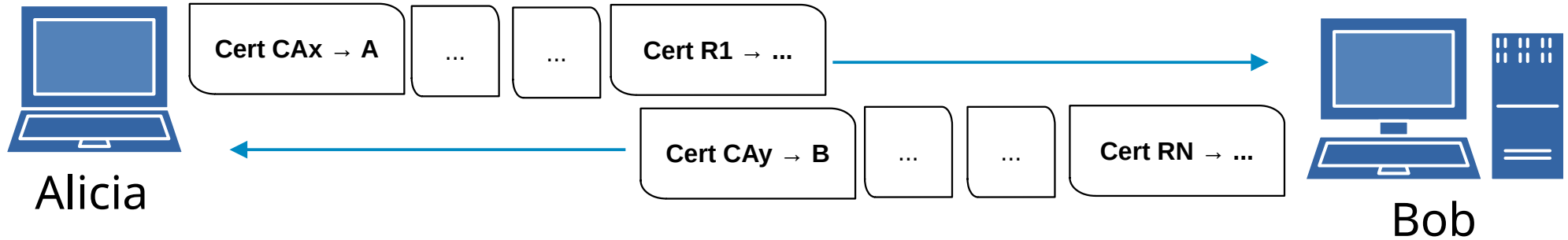
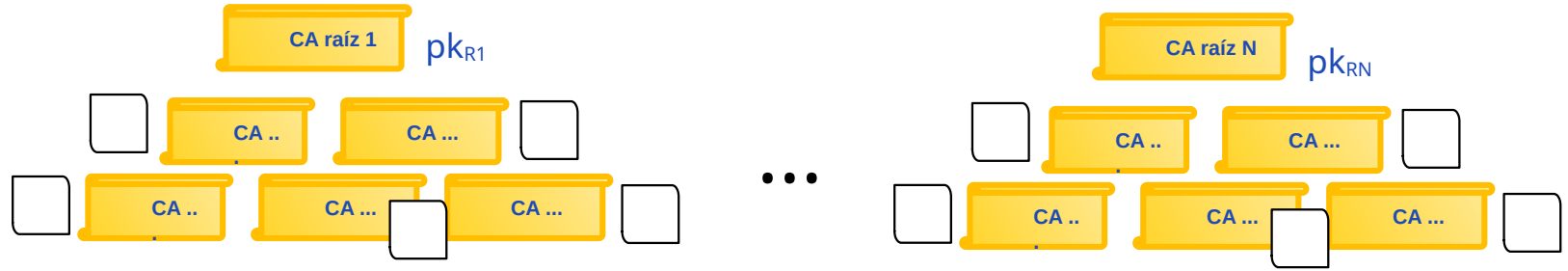


Bob

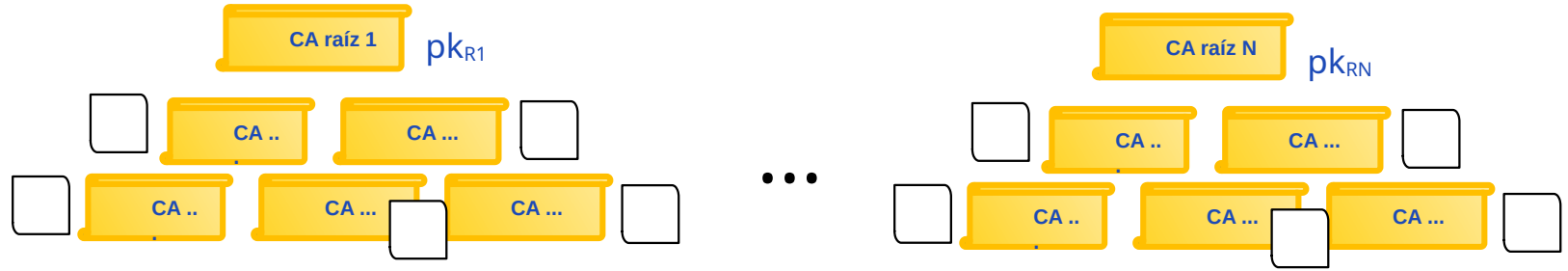
Casi real



Casi real



Casi real



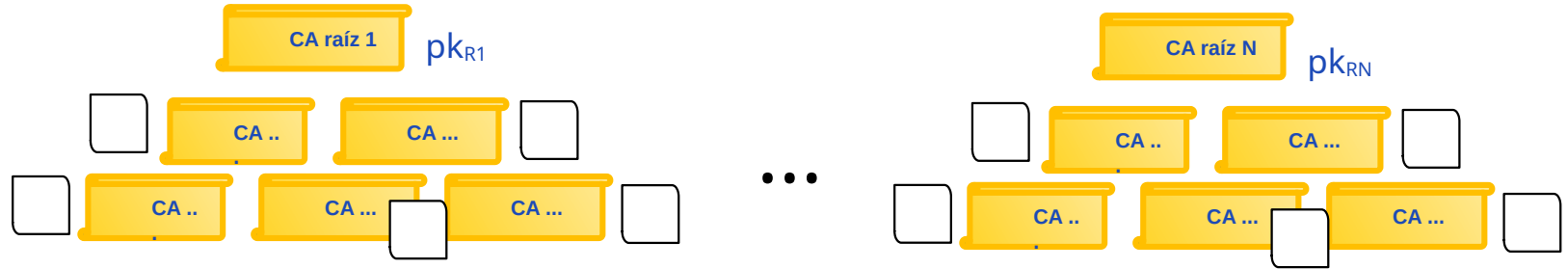
Alicia

Si todo salió bien con los CA,
Intercambio de claves de PKE con firma
Mensajes cifrados on IND-CCA PKE



Bob

Casi real



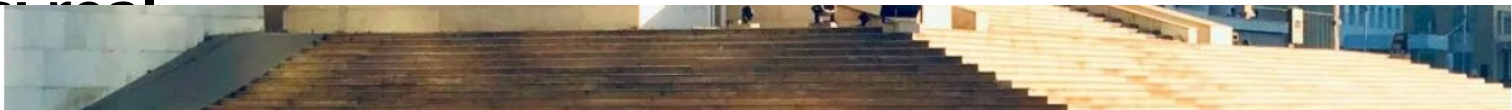
- Muchas autoridades, certificados de raíz integrados en el sistema operativo y/o en el browser
- Relativamente fácil autenticarse con un CA y obtener un certificado
- Muchos CA donde un adversario podría infiltrarse y generar un certificado fraudulento
 - Podría robar la identidad de Bob



Alicia



Bob



MONGOLIA

Catalin Cimpanu

June 30th, 2021

Government

Nation-state

News



Get more insights with the
Recorded Future
Intelligence Cloud.

[Learn more.](#)



Alicia

Mongolian certificate authority hacked eight times, compromised with malware

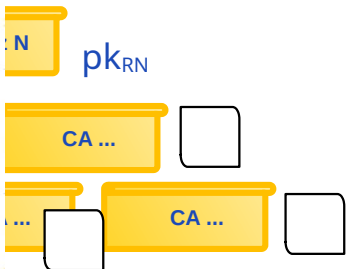
Hackers have breached a server belonging to **MonPass**, one of Mongolia's largest certificate authorities (CA), and have backdoored the company's official client with a Cobalt Strike-based backdoor.

The backdoor was active inside the company's official certificate installer app **between February 8 and March 3 this year**, security firm Avast said in a **report** today.

Incident has the hallmarks of a cyber-espionage campaign

The security breach came to light in late March when Avast discovered the backdoored installer and backdoor on one of its customers' systems.

- muchos CA donde un adversario podría infiltrarse y generar un certificado fraudolento
- Podría robar la identidad de Bob

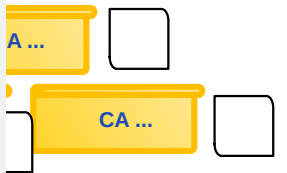


Bob

Continued



pk_{RN}



- Podria robar la identidad de Bob

Alicia



Bob

Continued



Alicia

Bob

Operation Black Tulip: Certificate authorities lose authority

DigiNotar, a digital certificate authority (CA), recently suffered a cyber-attack which led to its bankruptcy. In the attack false certificates were created for hundreds of websites, including Google and Skype. Once the incident was made public, the Dutch government and browser vendors took steps to limit the impact of the attack. But Fox-IT suggests in their [investigation report](#) that the cyber-attack had already started in mid-June and that for almost two months false certificates were used to eavesdrop on email and web browsing in Iran. We see three major issues:

1. **No immediate incident reporting:** DigiNotar did not immediately report the cyber-attack to customers or government authorities, which put the security and privacy of millions of citizens at risk. Immediate reporting of the incident and a swift response would have limited the impact considerably.
2. **Fundamental weaknesses in the design of HTTPS:** In the current setup, browsers and operating systems (e.g. Microsoft's certificate store) place trust by default in a large number of CAs (hundreds) by default, so a failure with one of them creates a risk for all users and all websites. The security of HTTPS equates to the security of the weakest CA. HTTPS should be modernized, to be more resilient against attacks and more user-friendly.
3. **Failure to implement basic security measures:** The Fox-IT report shows that basic security measures were not taken¹. It is imperative that service providers, like CAs, which play such a critical role in today's digital society, adhere to best practices. The attack highlights the importance of enforcing basic security best practices.

Alicia

Bob



ITL BULLETIN FOR JULY 2012

Preparing for and Responding to Certification Authority Compromise and Fraudulent Certificate Issuance

Paul Turner, Venafi

William Polk, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce

Elaine Barker, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce

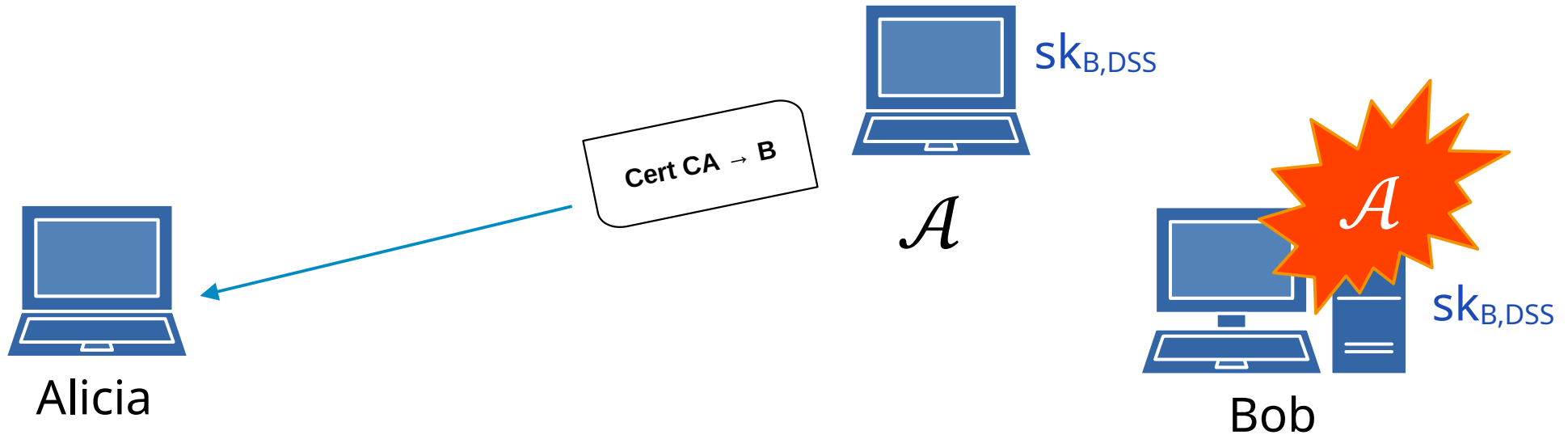
Today's digital society, adhere to best practices. The attack highlights the importance of enforcing basic security best practices.

DOU

Retirar certificados

Autoridad de certificación (CA)
Lista de claves publicas verificadas

- $pk_{A,DSS}$
- $pk_{B,DSS}$



Revocación de certificados

- En el caso de que una clave secreta venga comprometida, es necesario revocar el certificado correspondiente
- Bob tendría que comunicarle al CA que su clave fue comprometida
- El CA tiene que “anunciar” que su certificado para $pk_{B,DSS}$ no es mas valido
- De que manera puede un CA anunciar revocación?

Solución 1: Certificate Revocation List

- El CA publica una lista de certificados con fecha máxima futura, pero ya no validos (CRL)
- Al recibir un certificado emitido por esa CA, Alice tiene que bajar la lista y chequear si el certificado se encuentra revocado
- Esto comporta bajar varios MB de datos por chequeo
 - En 2017 se propone CRLite, un sistema muy interesante de compresión de CRLs
 - En 2025 Mozilla publica un diseño más compacto, con la intención de desplegarlo
- Si no se encuentra la CRL, Alicia tiene que decidir si confiar del certificado (exponiéndose a un ataque) o no aceptarlo (exponiéndose a un ataque de *denial of service*)

Solución 2: Online Certificate Status Protocol

- El sistema OCSP requiere que el CA presente un oráculo para chequear si un certificado en particular es aun valido
- Este sistema no requiere que el usuario baje varios MB de CRL
- Pero le requiere al CA de contestar muchas *queries* OCSP
- OCSP también implica que Alice *leakée* al CA que quiere comunicarse con Bob

Solución 2: OCSP stapling

- Una versión mas popular de OSCP requiere que el chequeo OCSP lo haga el propietario del certificado, Bob
- La salida del oráculo OCSP viene firmada por el CA junto a un *timestamp*
- Al proponer su clave publica y certificado, Bob también propone una salida OCSP reciente que confirma que el certificado es aun valido
- Esto reduce los leak de privacidad hacia el CA y también reduce las *queries* al CA
- Si el *timestamp* es muy generoso, una clave secreta podría ser vulnerada durante el periodo de validez de la salida OCSP...

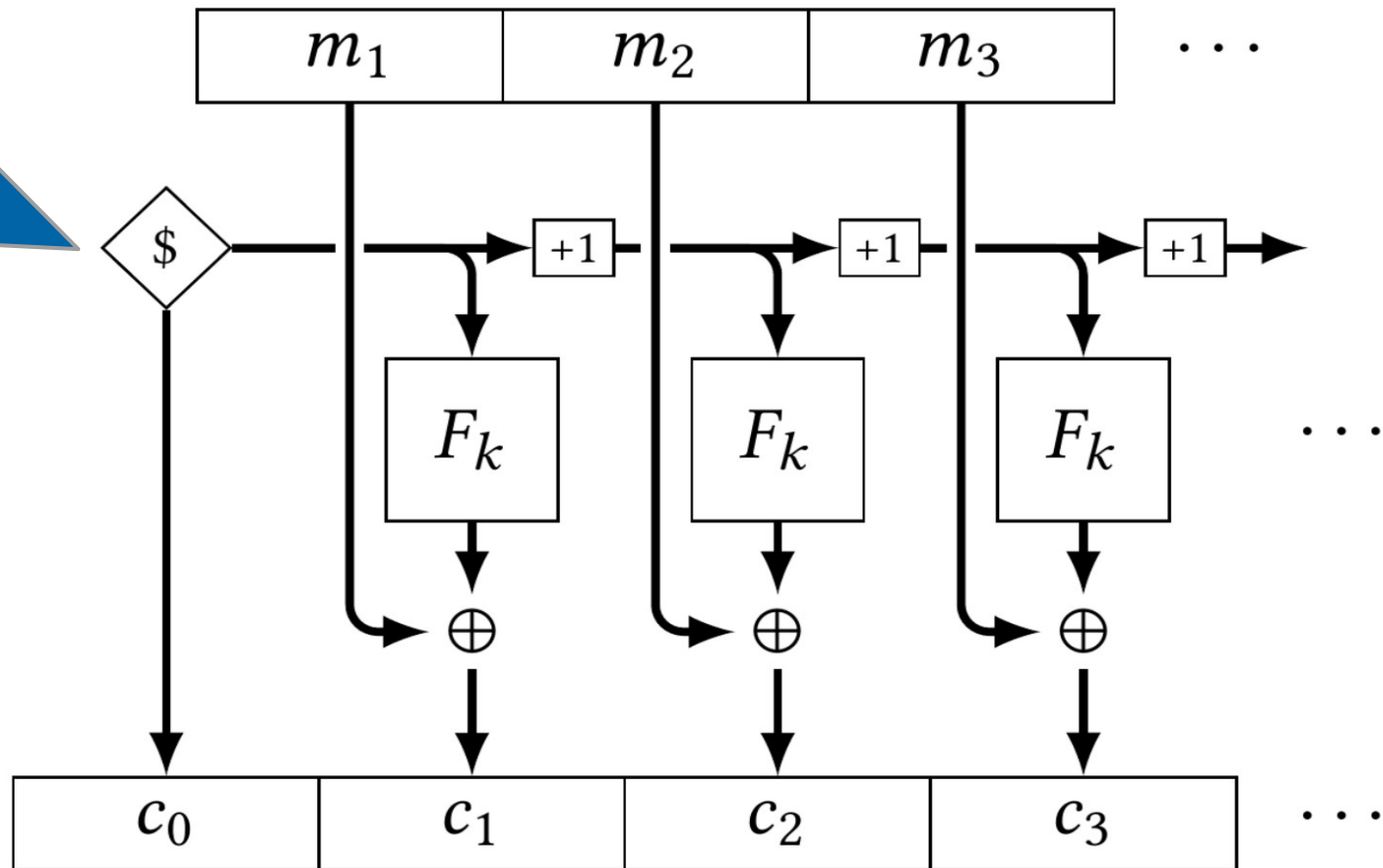
No Free Lunch

- El OTP nos presenta de entrada el problema de como compartir claves
- Vimos muchas construcciones que aumentan seguridad oferta por los sistemas de cifrado, compartiendo una sola clave (IND-CPA, AE)
- El cifrado de clave publica nos permite reducir el numero de partes con las cuales es necesario compartir claves (de “cualquiera” a “los CA raíz”)
- También nos permite reducir la cantidad de información “secreta” necesaria para comunicar de manera segura
- Pero el requisito de compartir algún tipo de información de manera autenticada queda
- Hoy en día esto lo hace los desarrolladores de sistemas operativos, navegadores, y las muchas “IT crowds” dentro de empresas

- Queda necesario confiar en varias partes
- Este problema es fundamental y ubicuo
 - También confiamos que la parte con la que comunicamos pueda mantener su sistema seguro
 - Y que nosotros podamos hacer lo mismo
 - Confiamos de poder implementar de manera correcta los sistemas criptográficos
 - O confiamos en el proveedor de librerías criptográficas
 - Confiamos en que las demostraciones matemáticas sean correctas, los postulados validos, los parámetros elegidos correctamente, y que los modelos de seguridad sean suficientemente amplios

Algorithm Substitution Attacks

- El valor inicial del contador es $\sim U(\{0,1\}^d)$
- Así mismo la clave $k \sim U(\{0,1\}^\lambda)$



- Supongamos un adversario que nos vende una implementación de AE que utiliza PRF-CTR
- Sea $k = k_1 k_2 \dots k_\lambda$ la clave secreta usada durante alguna "sesión"
- Al momento de cifrar m_i , en lugar de muestrear el contador $c_{0,i} \sim U(\{0,1\}^d)$, la implementación genera $c_{0,i} = U(\{0,1\}^{d-1}) \parallel k_i$
- La distribución de los cifrados parece legítima, pero leakea la clave secreta a lo largo de λ mensajes

- Este es un problema de interés académico



"algorithm substitution attacks" 

Articles About 197 results (0.10 sec)

Any time

Since 2024

Since 2023

Since 2020

Custom range...

Sort by relevance

Sort by date

Any type

Review articles

☐ include patents

☒ include citations

 Create alert

Algorithm substitution attacks from a steganographic perspective [PDF] acm.org

[S Berndt](#), [M Liśkiewicz](#) - Proceedings of the 2017 ACM SIGSAC ..., 2017 - dl.acm.org

... We will thus generalize the **algorithm substitution attacks** described in the literature to the setting, where the substituted algorithm also takes a message am as argument and the goal of ...

[☆ Save](#) [🔗 Cite](#) [Cited by 40](#) [Related articles](#) [All 6 versions](#)

Algorithm substitution attacks against receivers [HTML] springer.com

[M Armour](#), [B Poettering](#) - International Journal of Information Security, 2022 - Springer

This work describes a class of Algorithm Substitution Attack (ASA) generically targeting the receiver of a communication between two parties. Our work provides a unified framework that ...

[☆ Save](#) [🔗 Cite](#) [Cited by 4](#) [Related articles](#) [All 8 versions](#)

ASAP: algorithm substitution attacks on cryptographic protocols [PDF] acm.org

[S Berndt](#), [J Wichelmann](#), [C Pott](#), [TH Traving...](#) - Proceedings of the ..., 2022 - dl.acm.org

... 2.2 **Algorithm Substitution Attacks** In this work, we consider **algorithm substitution attacks** ...

For the sake of simplicity, we only consider **algorithm substitution attacks** against party A , ...

[☆ Save](#) [🔗 Cite](#) [Cited by 13](#) [Related articles](#) [All 5 versions](#)

Practical Algorithm Substitution Attacks on Real-World Public-Key Cryptosystems [PDF] ieee.org

[H Jiang](#), [J Han](#), [Z Zhang](#), [Z Ma...](#) - IEEE Transactions on ..., 2023 - ieeeexplore.ieee.org

... Liśkiewicz, "**Algorithm substitution attacks** from a steganographic perspective," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS ...

[☆ Save](#) [🔗 Cite](#) [Cited by 1](#) [Related articles](#) [All 2 versions](#)

Self-guarding cryptographic protocols against **algorithm substitution attacks** [PDF] ieee.org

[M Fischlin](#), [S Mazaheri](#) - 2018 IEEE 31st Computer Security ..., 2018 - ieeeexplore.ieee.org

... Abstract—We put forward the notion of self-guarding cryptographic protocols as a countermeasure to **algorithm substitution attacks**. Such self-guarding protocols can prevent ...

[☆ Save](#) [🔗 Cite](#) [Cited by 49](#) [Related articles](#) [All 6 versions](#)

Substitution attacks against message authentication [PDF] iacr.org

[M Armour](#), [B Poettering](#) - Cryptology ePrint Archive, 2019 - eprint.iacr.org

... This work introduces **Algorithm Substitution Attacks** (ASAs) on message authentication schemes. In light of revelations concerning mass surveillance, ASAs were initially introduced by ...

[☆ Save](#) [🔗 Cite](#) [Cited by 21](#) [Related articles](#) [All 8 versions](#) [🔗](#)

- Pero también practico

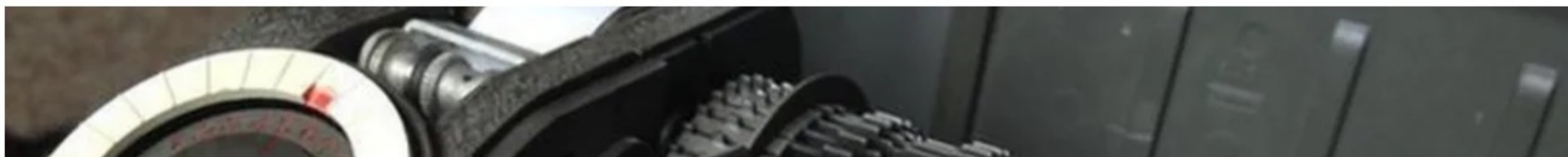


[Home](#) [News](#) [Sport](#) [Business](#) [Innovation](#) [Culture](#) [Travel](#) [Earth](#) [Video](#) [Live](#)

Swiss machines 'used to spy on governments for decades'

11 February 2020

Share



- Pero tambien practico



Homepage

Crypto

Spy radio

Burst encoders



Crypto Museum
cryptomuseum.com

Crypto AG

CIA

BND

NSA

ZfCh

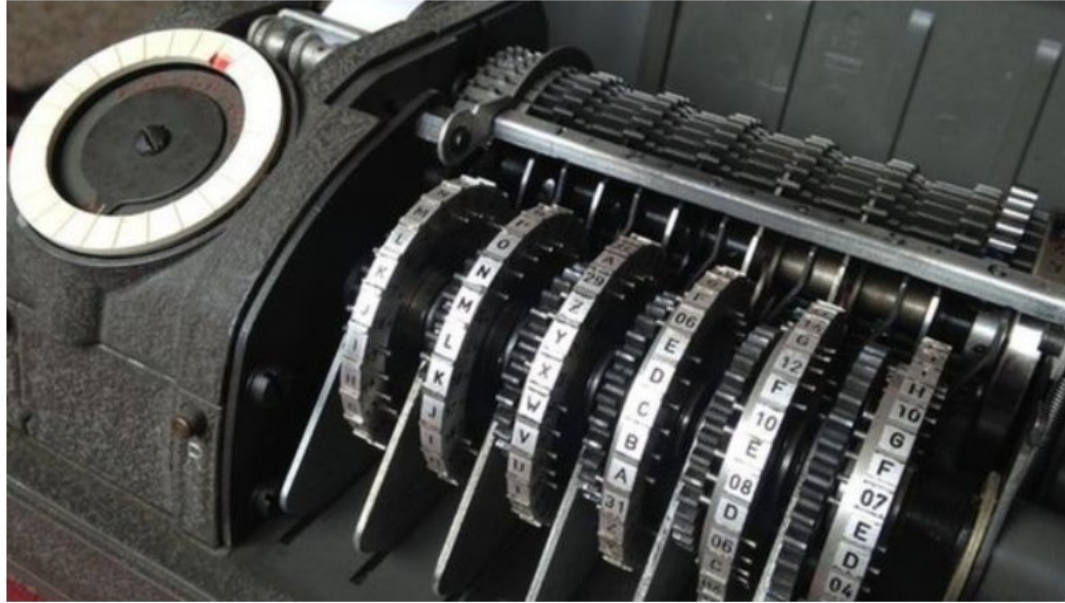
Gentleman's Agreement →

Operation RUBICON THESAURUS

The secret purchase of Crypto AG by BND and CIA

THESAURUS ¹ (later: RUBICON), was a secret operation of the German [Bundesnachrichtendienst \(BND\)](#) and the US [Central Intelligence Agency \(CIA\)](#), to purchase the Swiss crypto manufacturer [Crypto AG \(Hagelin\)](#) — codenamed **MINERVA** — in order to control the company, its algorithms and – indirectly – its customers. From **12 June 1970** ² onwards, Crypto AG was jointly owned by [CIA](#) and [BND](#), each with 50% of the shares, and from **30 June 1994** exclusively by the [CIA](#) [1].

The CIA's 'Minerva' Secret



CX52

Operation Condor Countries Used Crypto AG Devices Without Realizing the CIA Owned the Company, National Security Archive Documents Reveal

Encryption revelations raise questions about U.S. official knowledge of Argentina "dirty war" atrocities, Chile's Letelier assassination, Southern Cone military dictatorships

Swiss encryption company secretly owned by U.S. and German intelligence agencies, according to records obtained by the German public broadcaster, ZDF and *Washington Post*

En Ekoparty



Hagelin HC-520

Máquina de cifrado de bolsillo fuera de línea con pantalla LCD desarrollada por Crypto AG en 1977 tanto para el ámbito civil como el militar. El algoritmo criptográfico utilizado por este equipo podía ser descifrado por NSA de los Estados Unidos. Su software, se ejecutaba sobre un procesador DEC PDP-8 de 12 bits con 6 Kb de RAM. Este equipo fue ampliamente utilizado en nuestro país durante la guerra de Malvinas.

No es todo un bajón

- Problemas de matemática y computación teórica muy interesantes se encuentran en este ámbito
- Así mismo el impacto de un buen proyecto puede ser muy grande
- Existe una comunidad interesada en privacidad y seguridad

No es todo un bien

The Moral Character of Cryptographic Work^{*}

Phillip Rogaway

Department of Computer Science
University of California, Davis, USA
rogaway@cs.ucdavis.edu

December 2015
(minor revisions March 2016)

Abstract. Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently *political* tool, and it confers on the field an intrinsically *moral* dimension. The Snowden revelations motivate a reassessment of the political and moral positioning

teórica muy

o

o puede ser muy

acidad y seguridad

No es todo un baion

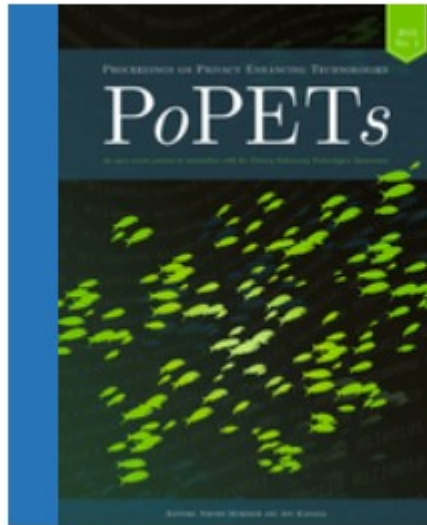
The Moral Character of Cryptographic Work*

Phillip Rogaway

Department of Computer Science
University of California, Davis, USA
rogaway@cs.ucdavis.edu

| teorica muy

:0



PETS 2024

The 24th Privacy Enhancing Technologies Symposium
July 15–20, 2024
Location: Bristol, UK

- Muchos puntos débiles se están reduciendo
- Sistemas de demostración de teoremas automáticos se están usando para encontrar y resolver bugs en la teoría
 - EasyCrypt y Tamarin
- Sistemas de verificación formal de implementaciones buscan reducir las chances de bugs y backdoors en las librerías crypto

- Con las nociones que vimos en el curso van a poder entender las ideas detrás de protocolos mas complicados
- Y que otorgan formas interesantes de seguridad
 - Un buen lugar para comenzar es <https://www.signal.org/docs/>
- Y hay mas primitivas para descubrir
 - Differential privacy,
 - Multiparty computation
 - Fully homomorphic encryption
 - Zero-knowledge proofs
 - ...

