Impacto del ataque *ROCA** en los certificados digitales emitidos por el RENIEC

Alvaro Cuno
Gerencia de Registros de Certificación Digital
21 de Agosto de 2018

[*ROCA = *The Return of Coppersmith Attack*]

Ley 27269

Ley de firmas y certificados digitales

8 de mayo del 2000

[16 artículos y 3 disposiciones

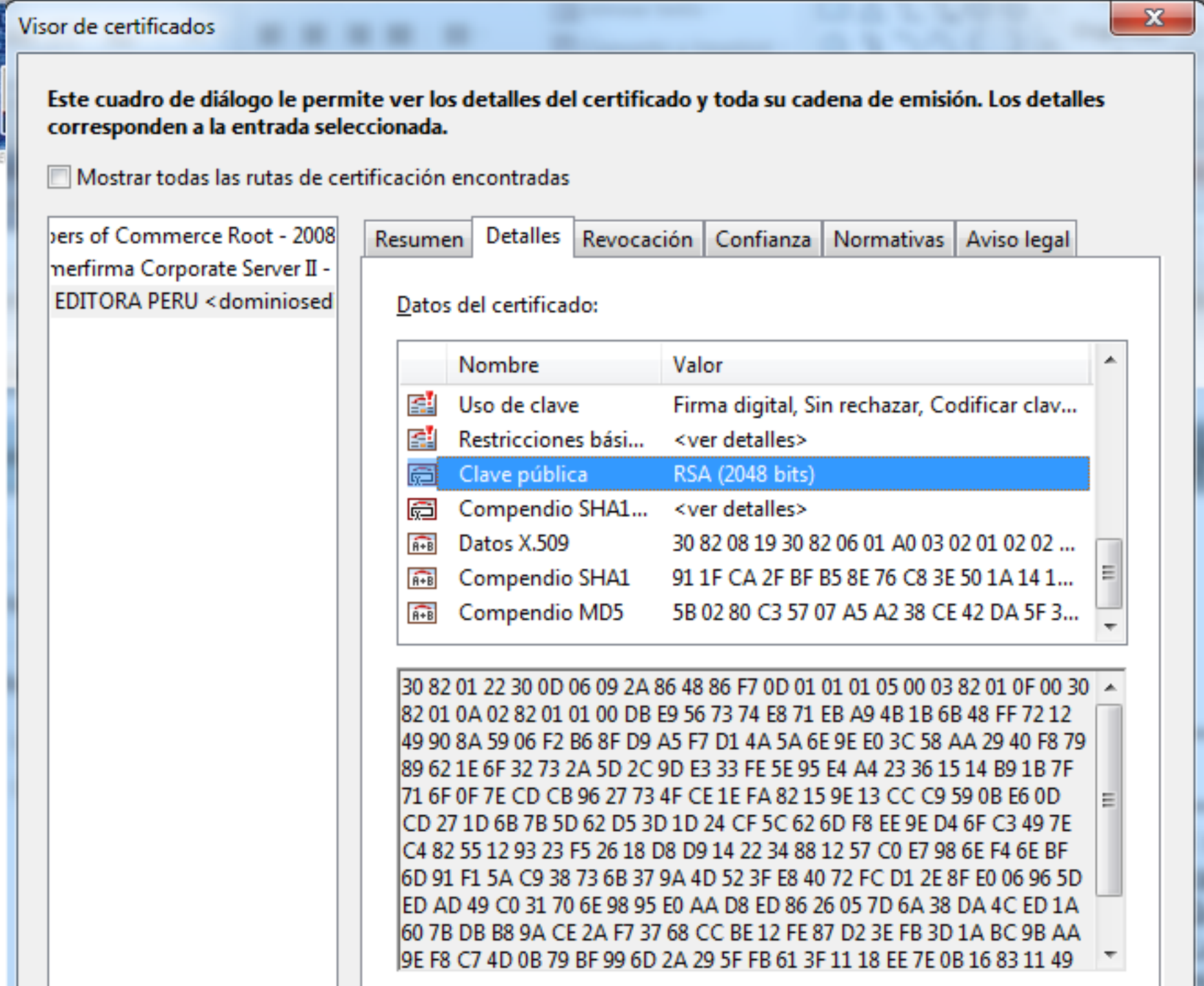
Artículo 3º Firma digital

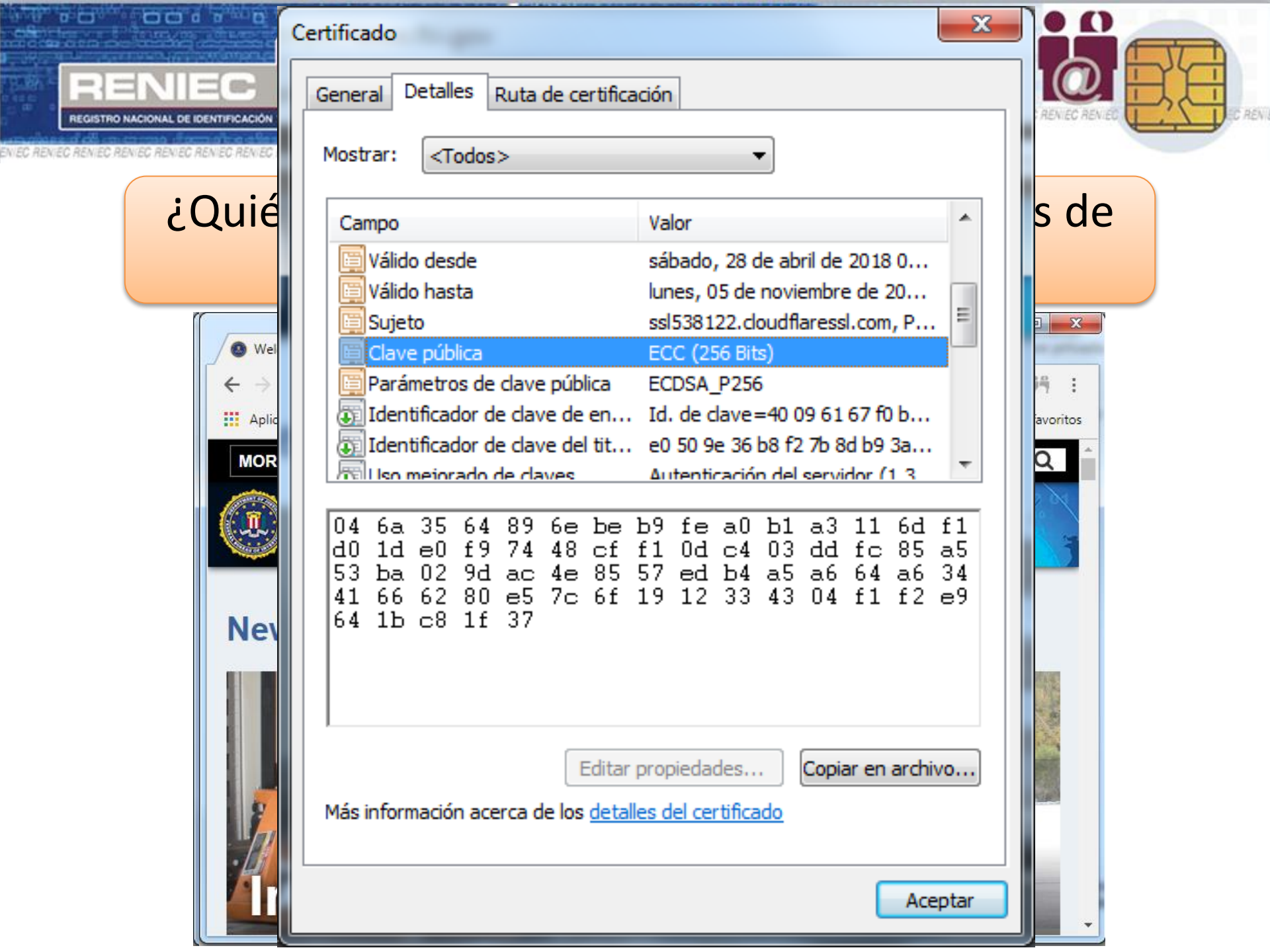
La firma digital es aquella **firma electrónica que utiliza una técnica de criptografía asimétrica**, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, **de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.**

Si las personas que conocen la llave pública pudieran derivar de ella la llave privada …

Escenarios de

Suplantación


Visor de certificados
Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.
Mostrar todas las rutas de certificación encontradas
ers of Commerce Root - 2008
nerfirma Corporate Server II -
EDITORA PERU <dominiosed
Resumen
Detalles
Revocación
Confianza
Normativas
Aviso legal
Datos del certificado:
Nombre
Valor
Uso de clave
Firma digital, Sin rechazar, Codificar clav...
Restricciones básí...
<ver detalles>
Clave pública
RSA (2048 bits)
Compendio SHA1...
<ver detalles>
Datos X.509
30 82 08 19 30 82 06 01 A0 03 02 01 02 02 ...
Compendio SHA1
91 1F CA 2F BF B5 8E 76 C8 3E 50 1A 14 1...
Compendio MD5
5B 02 80 C3 57 07 A5 A2 38 CE 42 DA 5F 3...
30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30
82 01 0A 02 82 01 01 00 DB E9 56 73 74 E8 71 EB A9 4B 1B 6B 48 FF 72 12
49 90 8A 59 06 F2 B6 8F D9 A5 F7 D1 4A 5A 6E 9E E0 3C 58 AA 29 40 F8 79
89 62 1E 6F 32 73 2A 5D 2C 9D E3 33 FE 5E 95 E4 A4 23 36 15 14 B9 1B 7F
71 6F 0F 7E CD CB 96 27 73 4F CE 1E FA 82 15 9E 13 CC C9 59 0B E6 0D
CD 27 1D 6B 7B 5D 62 D5 3D 1D 24 CF 5C 62 6D F8 EE 9E D4 6F C3 49 7E
C4 82 55 12 93 23 F5 26 18 D8 D9 14 22 34 88 12 57 C0 E7 98 6E F4 6E BF
6D 91 F1 5A C9 38 73 6B 37 9A 4D 52 3F E8 40 72 FC D1 2E 8F E0 06 96 5D
ED AD 49 C0 31 70 6E 98 95 E0 AA D8 ED 86 26 05 7D 6A 38 DA 4C ED 1A
60 7B DB B8 9A CE 2A F7 37 68 CC BE 12 FE 87 D2 3E FB 3D 1A BC 9B AA
9E F8 C7 4D 0B 79 BF 99 6D 2A 29 5F FB 61 3F 11 18 EE 7E 0B 16 83 11 49


RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN
¿Quié
s de
Certificado
General
Detalles
Ruta de certificación
Mostrar:
<Todos>
Campo
Valor
Válido desde
sábado, 28 de abril de 2018 0...
Válido hasta
lunes, 05 de noviembre de 20...
Sujeto
ssl538122.cloudflaressl.com, P...
Clave pública
ECC (256 Bits)
Parámetros de clave pública
ECDSA_P256
Identificador de clave de en...
Id. de clave=40 09 61 67 f0 b...
Identificador de clave del tit...
e0 50 9e 36 b8 f2 7b 8d b9 3a...
Uso mejorado de claves
Autenticación del servidor (1.3
04 6a 35 64 89 6e be b9 fe a0 b1 a3 11 6d f1
d0 1d e0 f9 74 48 cf f1 0d c4 03 dd fc 85 a5
53 ba 02 9d ac 4e 85 57 ed b4 a5 a6 64 a6 34
41 66 62 80 e5 7c 6f 19 12 33 43 04 f1 f2 e9
64 1b c8 1f 37
Editar propiedades...
Copiar en archivo...
Más información acerca de los detalles del certificado
Aceptar

¿Qué hacemos para que las personas que conocen la llave pública no puedan derivar de ella la llave privada?

Llaves de gran tamaño

Las tres (03) jerarquías de certificación del RENIEC utilizan llaves RSA de **2048 y 4096 bits** de longitud

Nivel	Entidad	Algoritmo de hash	Algoritmo de firma	Longitud de llaves (bits)
1	ECERNEP	SHA-512	RSAwithSHA512	4096
2	ECEP-X-offline	SHA-512	RSAwithSHA512	4096
	EC-PSVA	SHA-512	RSAwithSHA512	4096
3	ECEP-X-online	SHA-512	RSAwithSHA512	4096
Entidad final	Clase 1, 2, 3, 4	SHA-256	RSAwithSHA256	2048
	PSVA-TSA-TSU	SHA-256	RSAwithSHA256	2048
	Para pruebas	SHA-256	RSAwithSHA256	2048

Orden de magnitud

1 millón = 1’000,000 = 10^6	→	20 bits
7.6 billones = 7.6 x 10^9	→	32 bits
10^{617}	→	2048 bits
10^{1234}	→	4096 bits

El ataque *ROCA* en las noticias

[09 NOV 2017] https://www.xataka.com/seguridad/la-seguridad-del-dni-electronico-comprometida-a-quien-afecta-por-que-y-como-solucionarlo

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Identidad digital

Estonia Invalidates Digital Certificates Over Crypto Crack

Unpatched Infineon Chip Peril as Researchers Speed Up Encryption Key Attack

Jeremy Kirk (jeremy_kirk) • November 8, 2017 0 Comments

Twitter Facebook LinkedIn Credit Eligible Get Permission

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

MORE TO COME —

Crippling crypto weakness opens millions of smartcards to cloning

Gemalto IDPrime.NET almost certainly isn't the only smartcard vulnerable to ROCA.

DAN GOODIN - 10/23/2017, 3:30 PM

Serious Crypto-Flaw Lets Hackers Recover Private RSA Keys Used in Billions of Devices

October 16, 2017 Swati Khandelwal

Cinco claves para entender por qué el Gobierno ha desactivado tu DNI electrónico

- Un fallo de seguridad obligó a la Dirección General de la Policía a suspender el certificado electrónico de todos los DNIs expedidos desde abril del 2015
- Con la ayuda de uno de los desarrolladores del primer DNIe, explicamos cómo funciona, qué ha pasado y, sobre todo, si nuestros datos están seguros

Desactivada la firma digital de los DNI electrónicos por un fallo de seguridad

La medida, que afecta a los expedidos desde abril del 2015, viene por un fallo en el chip del fabricante

El problema está en un protocolo de transacciones digitales que utilizan millones de máquinas

Carmen Jané
Barcelona - Jueves, 09/11/2017 | Actualizado el 10/11/2017 a las 18:00 CET

7

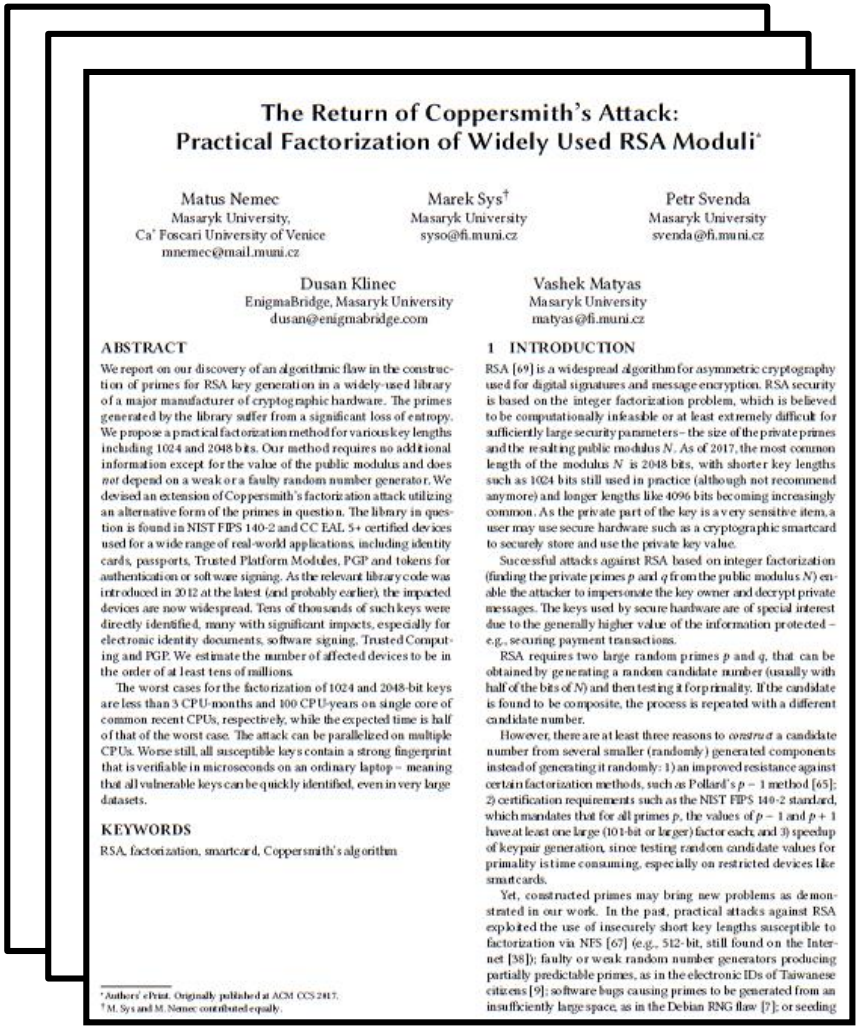
Medios nacionales

El omnipresente cifrado asimétrico de Rivest-Shamir-Adleman (RSA) se ha visto constantemente atacado desde su introducción en 1977. A lo largo de los años, se ha debilitado con éxito y ha mejorado muchas veces. La vulnerabilidad recientemente descubierta del Retorno del Ataque Cobre (ROCA) en octubre del 2017, que fue una implementación débil de la generación del *keypair* de RSA en los *chips* del Módulo de plataforma confiable (TPM) de Infineon, miles de millones de dispositivos de seguridad impactados, incluidas las tarjetas inteligentes.

Esta vulnerabilidad anunciada tenía a casi todas las grandes compañías del mundo luchando para analizar sus sistemas criptográficos confiables, y reemplazar las tarjetas inteligentes vulnerables en muy poco tiempo. Si no está familiarizado con el problema ROCA, simplemente entienda que se trata de un problema sísmico y que probablemente aún se utilicen miles de millones de dispositivos y tarjetas inteligentes vulnerables que ofrecen muy poca protección.

El ataque *ROCA*

The Return Of Coppersmith's Attack



The Return of Coppersmith's Attack:
Practical Factorization of Widely Used RSA Moduli*

Matus Nemec
Masaryk University,
Ca' Foscari University of Venice
mnemec@mail.muni.cz

Marek Sys†
Masaryk University
syso@fi.muni.cz

Petr Svenda
Masaryk University
svenda@fi.muni.cz

Dusan Klinec
EnigmaBridge, Masaryk University
dusan@enigmabridge.com

Vashek Matyas
Masaryk University
matyas@fi.muni.cz

ABSTRACT

We report on our discovery of an algorithmic flaw in the construction of primes for RSA key generation in a widely-used library of a major manufacturer of cryptographic hardware. The primes generated by the library suffer from a significant loss of entropy. We propose a practical factorization method for various key lengths including 1024 and 2048 bits. Our method requires no additional information except for the value of the public modulus and does *not* depend on a weak or a faulty random number generator. We devised an extension of Coppersmith's factorization attack utilizing an alternative form of the primes in question. The library in question is found in NIST FIPS 140-2 and CC EAL 5+ certified devices used for a wide range of real-world applications, including identity cards, passports, Trusted Platform Modules, PGP and tokens for authentication or software signing. As the relevant library code was introduced in 2012 at the latest (and probably earlier), the impacted devices are now widespread. Tens of thousands of such keys were directly identified, many with significant impacts, especially for electronic identity documents, software signing, Trusted Computing and PGP. We estimate the number of affected devices to be in the order of at least tens of millions.

The worst cases for the factorization of 1024 and 2048-bit keys are less than 3 CPU-months and 100 CPU-years on single core of common recent CPUs, respectively, while the expected time is half of that of the worst case. The attack can be parallelized on multiple CPUs. Worse still, all susceptible keys contain a strong fingerprint that is verifiable in microseconds on an ordinary laptop – meaning that all vulnerable keys can be quickly identified, even in very large datasets.

KEYWORDS

RSA, factorization, smartcard, Coppersmith's algorithm

1 INTRODUCTION

RSA [69] is a widespread algorithm for asymmetric cryptography used for digital signatures and message encryption. RSA security is based on the integer factorization problem, which is believed to be computationally infeasible or at least extremely difficult for sufficiently large security parameters – the size of the private primes and the resulting public modulus N. As of 2017, the most common length of the modulus N is 2048 bits, with shorter key lengths such as 1024 bits still used in practice (although not recommend anymore) and longer lengths like 4096 bits becoming increasingly common. As the private part of the key is a very sensitive item, a user may use secure hardware such as a cryptographic smartcard to securely store and use the private key value.

Successful attacks against RSA based on integer factorization (finding the private primes p and q from the public modulus N) enable the attacker to impersonate the key owner and decrypt private messages. The keys used by secure hardware are of special interest due to the generally higher value of the information protected – e.g., securing payment transactions.

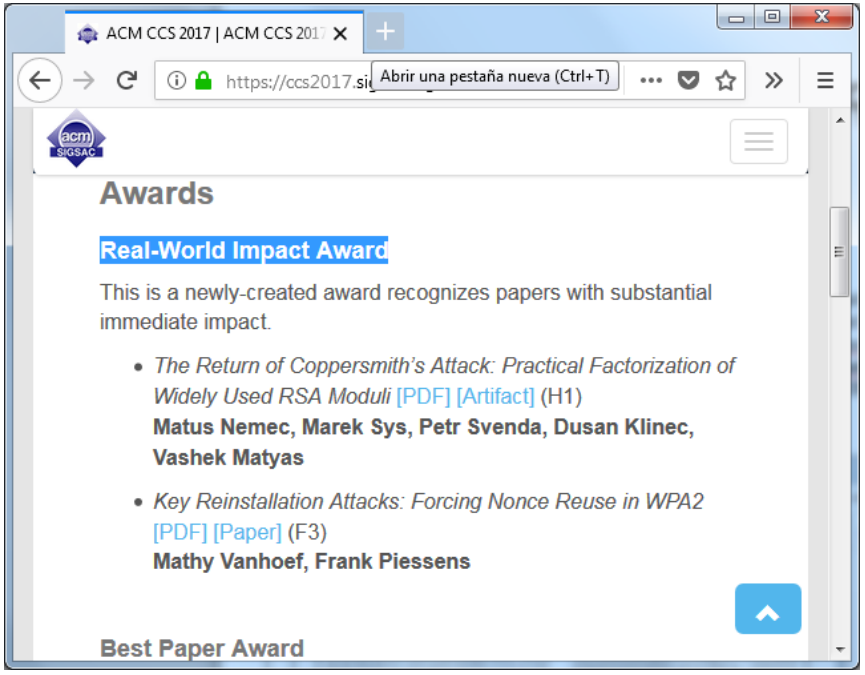
RSA requires two large random primes p and q, that can be obtained by generating a random candidate number (usually with half of the bits of N) and then testing it for primality. If the candidate is found to be composite, the process is repeated with a different candidate number.

However, there are at least three reasons to *construct* a candidate number from several smaller (randomly) generated components instead of generating it randomly: 1) an improved resistance against certain factorization methods, such as Pollard's $p-1$ method [65]; 2) certification requirements such as the NIST FIPS 140-2 standard, which mandates that for all primes p, the values of $p-1$ and $p+1$ have at least one large (101-bit or larger) factor each; and 3) speedup of keypair generation, since testing random candidate values for primality is time consuming, especially on restricted devices like smartcards.

Yet, constructed primes may bring new problems as demonstrated in our work. In the past, practical attacks against RSA exploited the use of insecurely short key lengths susceptible to factorization via NFS [67] (e.g., 512-bit, still found on the Internet [38]); faulty or weak random number generators producing partially predictable primes, as in the electronic IDs of Taiwanese citizens [9]; software bugs causing primes to be generated from an insufficiently large space, as in the Debian RNG flaw [7]; or seeding

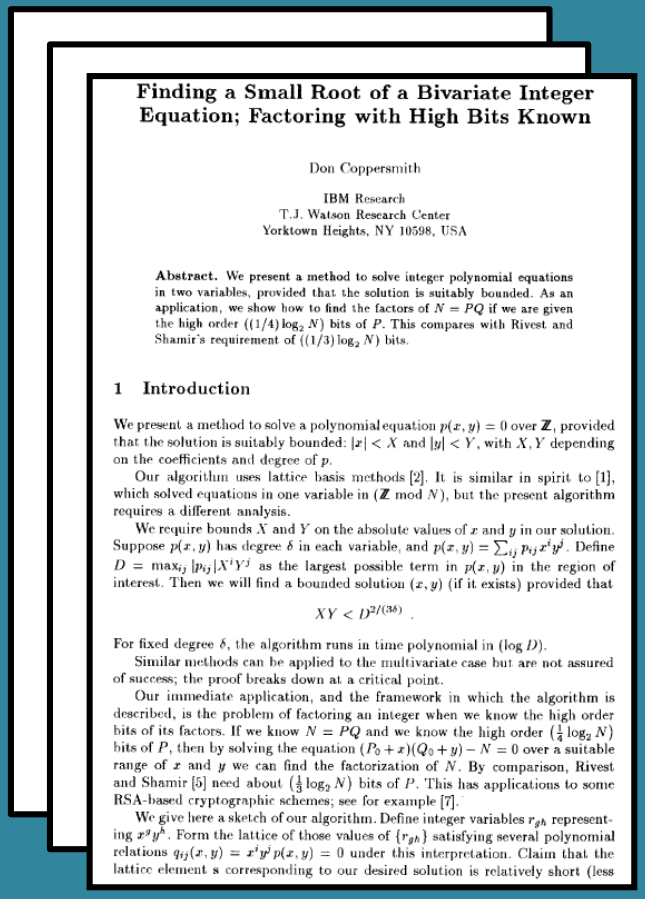
* Authors' ePrint. Originally published at ACM CCS 2017.
† M. Sys and M. Nemec contributed equally.

M. Nemec, M. Sys, P. Svenda, D. Klinec and V. Matyas. *The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli*. **24th ACM Conference on Computer and Communications Security (CCS'2017)**. 1631-1648. **2017**, Oct. ACM.



El ataque *ROCA*

El ataque de Coppersmith



Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known

Don Coppersmith

IBM Research
T.J. Watson Research Center
Yorktown Heights, NY 10598, USA

Abstract. We present a method to solve integer polynomial equations in two variables, provided that the solution is suitably bounded. As an application, we show how to find the factors of $N = PQ$ if we are given the high order $((1/4)\log_2 N)$ bits of P. This compares with Rivest and Shamir's requirement of $((1/3)\log_2 N)$ bits.

1 Introduction

We present a method to solve a polynomial equation $p(x, y) = 0$ over $\mathbb{Z}$, provided that the solution is suitably bounded: $|x| < X$ and $|y| < Y$, with X, Y depending on the coefficients and degree of p.

Our algorithm uses lattice basis methods [2]. It is similar in spirit to [1], which solved equations in one variable in ($\mathbb{Z}$ mod N), but the present algorithm requires a different analysis.

We require bounds X and Y on the absolute values of x and y in our solution. Suppose $p(x, y)$ has degree δ in each variable, and $p(x, y) = \sum_{ij} p_{ij} x^i y^j$. Define $D = \max_{ij} |p_{ij}| X^i Y^j$ as the largest possible term in $p(x, y)$ in the region of interest. Then we will find a bounded solution (x, y) (if it exists) provided that

$$XY < D^{2/(3\delta)} .$$

For fixed degree δ, the algorithm runs in time polynomial in $(\log D)$.

Similar methods can be applied to the multivariate case but are not assured of success; the proof breaks down at a critical point.

Our immediate application, and the framework in which the algorithm is described, is the problem of factoring an integer when we know the high order bits of its factors. If we know $N = PQ$ and we know the high order $(\frac{1}{4}\log_2 N)$ bits of P, then by solving the equation $(P_0 + x)(Q_0 + y) - N = 0$ over a suitable range of x and y we can find the factorization of N. By comparison, Rivest and Shamir [5] need about $(\frac{1}{3}\log_2 N)$ bits of P. This has applications to some RSA-based cryptographic schemes; see for example [7].

We give here a sketch of our algorithm. Define integer variables r_{gh} representing $x^g y^h$. Form the lattice of those values of $\{r_{gh}\}$ satisfying several polynomial relations $q_{ij}(x, y) = x^i y^j p(x, y) = 0$ under this interpretation. Claim that the lattice element $\mathbf{s}$ corresponding to our desired solution is relatively short (less

D. Coppersmith. *Finding a small root of a bivariate integer equation; factoring with high bits known.* **International Conference on the Theory and Applications of Cryptographic Techniques.** Springer, Berlin, Heidelberg, **1996**.

"El conocimiento parcial de una llave pública permite calcular la correspondiente llave privada."

Algoritmo de generación de llaves RSA

Versión didáctica

1. Se seleccionan dos números primos aleatorios, a los que denominaremos p y q

2. Se calcula $N = p*q$ y $\phi(N)=(p-1)(q-1)$

3. Se elige un exponente público $e<\phi(N)$

4. Se calcula el exponente privado $d = e^{-1} \ mod \ \phi(N)$

Al par ***(e, N)*** se le denomina la llave pública, donde N es un número de gran tamaño y ***e*** usualmente es igual a 65,537.

Al par ***(d, N)*** se le denomina la llave privada , donde d depende de p y q, los cuales son los factores primos de N.

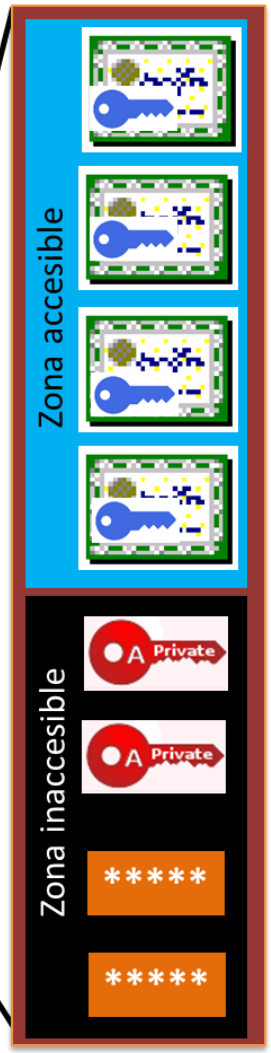
DNIe peruano

- Chip SmartMX de NXP
- Common Criteria EAL5+
- FIPS 140-2 nivel 3
- Memoria EEPROM de 144K

ICAO

MoC

PKI



Estructura PKCS#15

Certificado raíz: ECERNEP

Certificado Intermedio: ECEP

Certificado de Firma Digital: CIUDADANO

Certificado de Autenticación: CIUDADANO

X509v3

Llave privada de Firma Digital — *Número entero de mas de **600 dígitos**. Desconocido por todos.*

Llave privada de Autenticación — *Número entero de mas de **600 dígitos**. Desconocido por todos.*

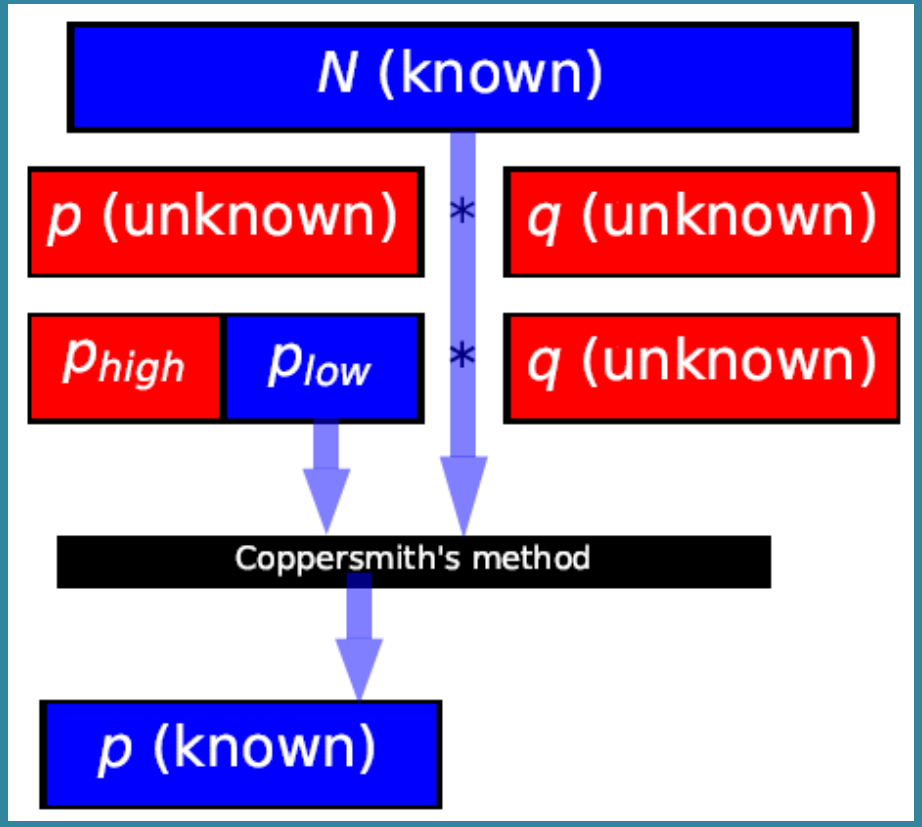
PIN 2 — *Número entero de 6 dígitos. Conocido solamente por el titular. Protege la llave privada de firma.*

PIN 1 — *Número entero de 6 dígitos. Conocido solamente por el titular. Protege la llave privada de autenticación.*

El ataque *ROCA*

El ataque de Coppersmith

1. Módulo
2. Factores desconocidos
3. Conocimiento parcial del primo *p*
4. Aplicar el ataque Coppersmith como una caja negra



El ataque *ROCA*

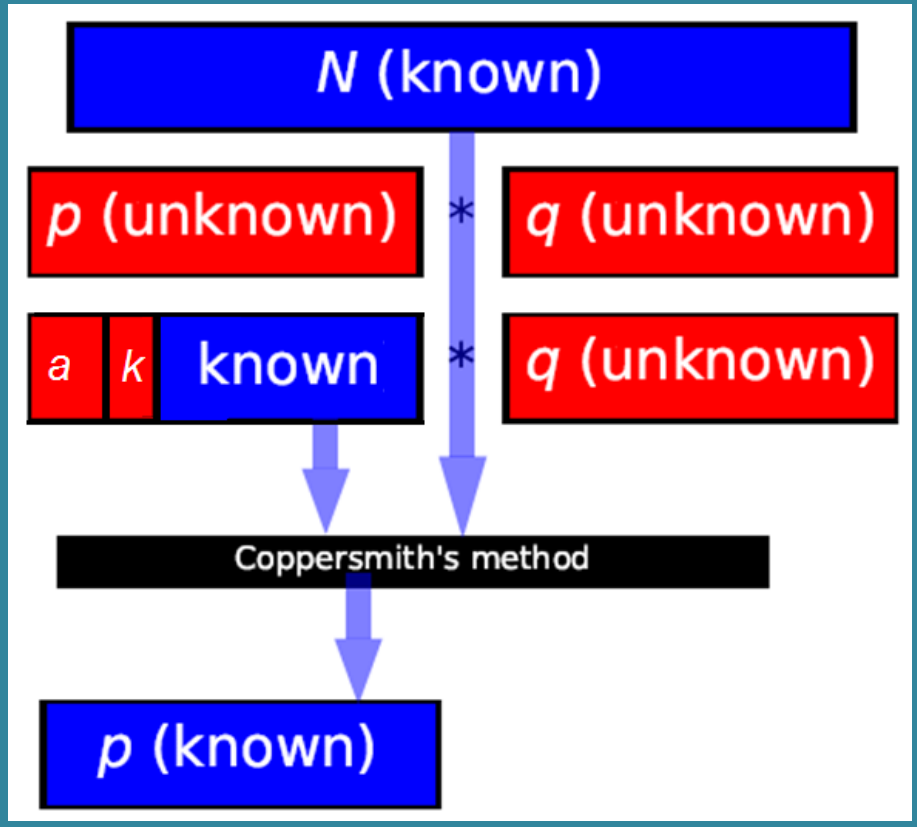
El regreso del ataque de Coppersmith

1. Módulo

2. Factores desconocidos

3. Conocimiento parcial del primo p, el cual obedece a una estructura reconocible

4. Aplicar el ataque Coppersmith como una caja negra



El ataque *ROCA*

$$N = p * q$$

$$p_{ideal} = \text{random prime} \qquad q_{ideal} = \text{random prime}$$

Números primos generados por Infineon Technologies AG

$$p_{vulnerable} = (k * M + 65537^a \bmod M);\ a, k \in \mathbb{Z}$$

$$M = 2 * 3 * 5 * 7 * \cdots * P_n$$

- *M* es el producto de n primos sucesivos (2, 3, 5, 7, 11, 13, ...) y *n* es una constante que solo depende del tamaño de la llave deseada

- Quedando como valores desconocidos únicamente los valores de *k* y *a*.

keysize	512	1024
n	39	71
a	62	256
k	37	54

El ataque *ROCA*: entropía

Entropía en un primo de 1024 bits

Random

1024 bits de entropía

Números primos generados por Infineon Technologies AG

Vulnerable

*310 bits de entropía**

Pérdida de entropía!!!

*Los investigadores han encontrado formas de reducir el tamaño de *a* y *k*

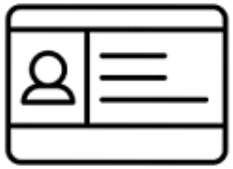
El ataque ROCA: tiempo

- Utilizando un computador de propósito general, la factorización de una llave **RSA de 2048 bits** generada correctamente tomaría varios **cuatrillones de años**.
- En cambio, factorizar una **llave RSA de 2048 bits** generada con el esquema "acelerado" de Infineon Technologies AG tomaría **100 años en el peor caso** y **50 años en promedio**.
- Sin embargo, este tiempo de factorización puede ser reducido notablemente distribuyendo el trabajo en una red de computadores.
  - Por ejemplo, utilizando **1000 computadores del servicio AWS** (Amazon Web Service), la factorización de una llave de 2048 bits con la vulnerabilidad ROCA tomaría **no más de 17 días y una inversión de aprox. 40 mil US$** (CERT-EU, 2018).

M. Nemec, M. Sys, P. Svenda, D. Klinec, V. Matyas: The Return of Coppersmith's Attack..., ACM CCS 2017

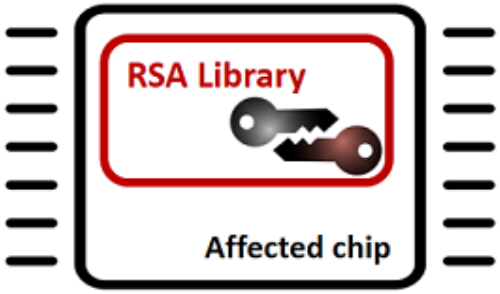
The usage domains affected by the vulnerable library

Identity documents
(eID, eHealth cards)



Trusted Platform Modules
(Data encryption, Platform integrity)

Software signing

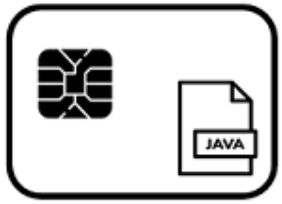


Secure browsing
(TLS/HTTPS*)

Authentication tokens

Message protection
(S-MIME/PGP)

Programmable smartcards



** only a small number of vulnerable keys found*

El ataque ROCA: impacto en Documentos de Identidad electrónicos

- De acuerdo a la Autoridad de los Sistemas de Información de Estonia (ISA, 2018) son 11 los países cuyos DNIe son vulnerables al ataque ROCA:
  - **Estonia (800 mil DNIe afectados),**
  - **España (17 millones de DNIe afectados),**
  - **Eslovaquia,**
  - **Austria,**
  - **Polonia,**
  - **Bulgaria,**
  - **Kosovo,**
  - **Italia,**
  - **Taiwan,**
  - **Brasil y**
  - **Malasia**

- **España** optó por revocar los certificados digitales de los DNIe afectados y solicitó a los ciudadanos realizar la renovación de sus certificados digitales de forma presencial.
- **Estonia** permitió que los ciudadanos afectados puedan actualizar sus certificados de forma remota vía Internet, y optaron por cambiar su sistema criptográfico RSA al basado en Curvas Elípticas (ECC).
- A la fecha, no se tiene información de la cantidad de DNIe afectados en los otros países debido a que no han difundido información pública al respecto.

El ataque ROCA: riesgo en la práctica

- El ataque ROCA permite factorizar una llave pública RSA teniendo acceso únicamente a un certificado digital.
- No es necesario que el atacante tenga acceso a la tarjeta DNIe ni tampoco al PIN de activación del ciudadano.
- Una vez factorizada la llave pública, el atacante puede calcular la llave privada del ciudadano.
- Obteniendo la llave privada, el atacante estaría en capacidad de firmar digitalmente en nombre del ciudadano (suplantación).
- Un ejemplo de este ataque en la práctica sería: si una persona A le envía un PDF con su firma digital a una persona B, ésta persona B, a partir del PDF firmado, podría obtener la llave privada de A y firmar documentos en nombre de A.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Identidad digital

El ataque ROCA: ¿Impacto en el DNIe peruano?

El ataque ROCA: ¿Impacto en el DNIe peruano?

El ataque ROCA: ¿Impacto en el DNIe peruano?

Condiciones para la vulnerabilidad ROCA

(1) Utilización del chip de la compañía *Infineon Technologies AG*

(2) Utilización de la librería RSALib versión 1.02.013

DNIe peruano

- Chip de contactos SmartMX del fabricante NXP Semiconductors, modelo P5CD144V0B

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Identidad digital

Dispositivos criptográficos homologados por el RENIEC

Fabricante: BitID
Modelo: iAm
Certificación: Common Criteria
Hardware: Reporte de certificación | Security Target
Firmware: Reporte de certificación | Security Target
Reporte de Homologación

Fabricante: BitID
Modelo: CryptoKey
Certificación: Common Criteria
Hardware: Reporte de certificación | Security Target
Firmware: Reporte de certificación | Security Target
Reporte de Homologación

Fabricante: BitID
Modelo: TouchASign 2048
Certificación: Common Criteria
Hardware: Reporte de certificación | Security Target
Firmware: Reporte de certificación | Security Target
Reporte de Homologación

Fabricante: SafeNet
Modelo: iKey 4000
Certificación: FIPS 140-2
Diploma: Único
Security Policy
Reporte de Homologación

Fabricante: Safelan
Modelo: eToken 5100
Certificación: FIPS 140-2
Diploma: Multiple
Security Policy
Reporte de Homologación

Fabricante: SafeNet
Modelo: eToken PRO (Java)
Certificación: FIPS 140-2
Diploma: Único
Security Policy
Reporte de Homologación

Fabricante: Feitian
Modelo: ePass 2003
Certificación: FIPS 140-2
Diploma: Multiple
Security Policy
Reporte de Homologación

Fabricante: Athena Smartcard
Modelo: IDProtect Key with LASER P60
Certificación: FIPS 140-2
Diploma: Multiple
Security Policy
Reporte de Homologación

Fabricante: Bit4ID
Modelo: tokenME
Certificación: FIPS 140-2
Diploma: Multiple
Security Policy
Reporte de Homologación

Fabricante: Sagem Orga
Modelo: ypsID
Certificación: FIPS 140-2
Diploma: Único
Security Policy
Reporte de Homologación

Fabricante: Cryptovision
Modelo: JCOP 2.4.2 R3
Certificación: Common Criteria
Hardware: Reporte de certificación | Security Target
Firmware: Reporte de certificación | Security Target
Applet: Reporte de certificación | Security Target
Reporte de Homologación

Fabricante: Bit4ID
Modelo: J-Sign
Certificación: Common Criteria
Hardware: Reporte de certificación | Security Target
Firmware: Reporte de certificación | Security Target
Applet: Reporte de certificación | Security Target
Reporte de Homologación

Fabricante: Longmai
Modelo: mToken CryptoID
Certificación: FIPS 140-2
Diploma: Multiple
Security Policy
Reporte de Homologación

Fabricante: Bit4ID
Modelo: tokenME v2
Certificación: FIPS 140-2
Diploma: Multiple
Security Policy
Reporte de Homologación

Fabricante: Bit4ID
Modelo: tokenME v3
Certificación: FIPS 140-2
Diploma: Multiple
Security Policy
Reporte de Homologación

Fabricante: Morpho Safran
Modelo: ypsID e-M Key
Certificación: FIPS 140-2
Diploma: Único
Security Policy
Reporte de Homologación

Fabricante: ACS
Modelo: ACR1011 SMicro (CCID)
Certificación: FIPS 140-2
Diploma: Único
Security Policy
Reporte de Homologación

Fabricante: ACS
Modelo: ACOS5-64
Certificación: FIPS 140-2
Diploma: Único
Security Policy
Reporte de Homologación

Fabricante: ACS
Modelo: CryptoMate Nano
Certificación: FIPS 140-2
Diploma: Único
Security Policy
Reporte de Homologación

Fabricante: Athena Smartcard
Modelo: IDProtect Key with LASER P60
Certificación: FIPS 140-2
Diploma: Multiple
Security Policy
Reporte de Homologación

Fabricante: SafeNet
Modelo: SafeNet eToken 5110
Certificación: FIPS 140-2
Diploma: Multiple
Security Policy
Reporte de Homologación

Fabricante: Feitian
Modelo: AudioPass
Certificación: FIPS 140-2
Diploma: Multiple
Security Policy
Reporte de Homologación

Fabricante: Bit4ID
Modelo: DigitalDNA
Certificación: Common Criteria
Hardware: Reporte de certificación | Security Target
Firmware: Reporte de certificación | Security Target
Applet: Reporte de certificación | Security Target
Reporte de Homologación

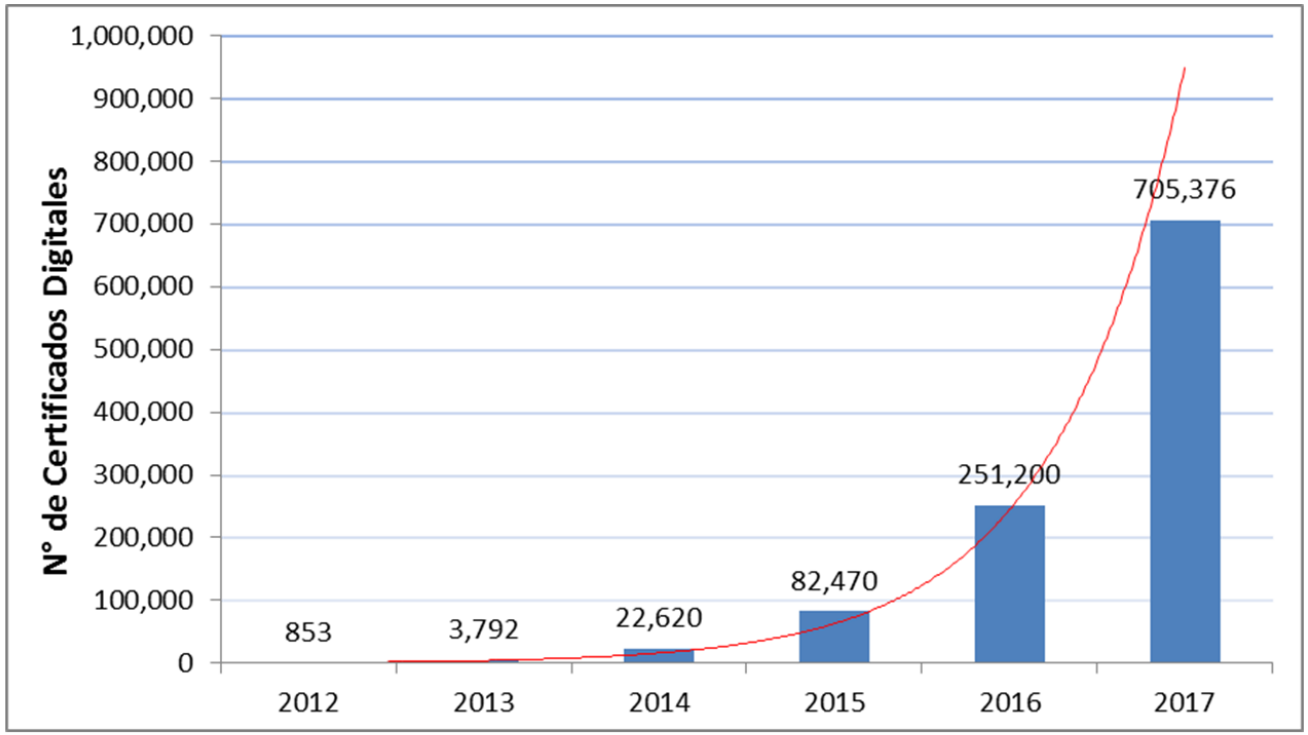
Fabricante: Bit4ID
Modelo: Crypto Java Card
Certificación: Common Criteria
Hardware: Reporte de certificación | Security
Firmware: Reporte de certificación | Security
Applet: Reporte de certificación | Security T
Reporte de Homologación

CDs de la PKI del Estado peruano

- BD de CDs emitidos por el RENIEC.
- Los CDs contienen llaves públicas RSA de 2048 bits

CD de la PKI del Estado peruano

- BD de CD emitidos por el RENIEC.
- Los CD contienen llaves públicas RSA de 2048 bits



En el caso del presente año, al 20JUN2018, los certificados digitales emitidos por el RENIEC ascienden a 498,174.

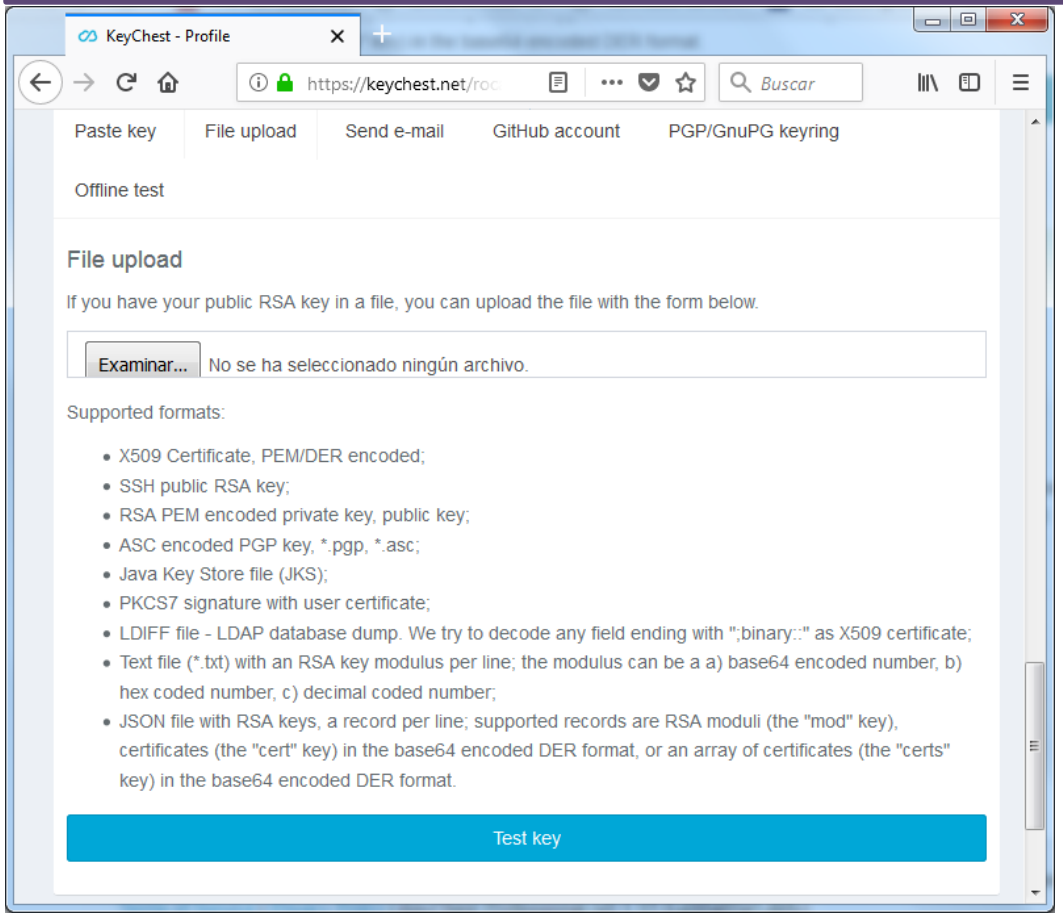
Impacto en los CD de la PKI del Estado

Fase 1: Análisis de los CD de Autoridad, los cuales cuentan con llaves RSA de 4096 bits

Jerarquía SHA-1	RENIEC Certification Authority	*The key is resistant to ROCA*
	RENIEC Class I CA	*The key is resistant to ROCA*
	RENIEC Class II CA	*The key is resistant to ROCA*
	RENIEC Class III CA	*The key is resistant to ROCA*
	RENIEC Class IV CA	*The key is resistant to ROCA*
	RENIEC Class V CA	*The key is resistant to ROCA*
	RENIEC Class VI CA	*The key is resistant to ROCA*
	RENIEC Time-Stamping Authority	*The key is resistant to ROCA*
Jerarquía SHA-256	RENIEC High Grade Certification Authority	*The key is resistant to ROCA*
	RENIEC Class I High Grade CA	*The key is resistant to ROCA*
	RENIEC Class II High Grade CA	*The key is resistant to ROCA*
	RENIEC Class III High Grade CA	*The key is resistant to ROCA*
	RENIEC Class IV High Grade CA	*The key is resistant to ROCA*
	RENIEC Class V High Grade CA	*The key is resistant to ROCA*
	RENIEC Class VI High Grade CA	*The key is resistant to ROCA*
	RENIEC High Grade Time-Stamping Authority	*The key is resistant to ROCA*

Impacto en los CD emitidos por el RENIEC

Fase 1: Análisis de los CD de Autoridad, los cuales cuentan con llaves RSA de 4096 bits



https://keychest.net/roca#/

Jerarquía SHA-1	RENIEC Certification Authority	*The key is resistant to ROCA*
	RENIEC Class I CA	*The key is resistant to ROCA*
	RENIEC Class II CA	*The key is resistant to ROCA*
	RENIEC Class III CA	*The key is resistant to ROCA*
	RENIEC Class IV CA	*The key is resistant to ROCA*
	RENIEC Class V CA	*The key is resistant to ROCA*
	RENIEC Class VI CA	*The key is resistant to ROCA*
	RENIEC Time-Stamping Authority	*The key is resistant to ROCA*
Jerarquía SHA-256	RENIEC High Grade Certification Authority	*The key is resistant to ROCA*
	RENIEC Class I High Grade CA	*The key is resistant to ROCA*
	RENIEC Class II High Grade CA	*The key is resistant to ROCA*
	RENIEC Class III High Grade CA	*The key is resistant to ROCA*
	RENIEC Class IV High Grade CA	*The key is resistant to ROCA*
	RENIEC Class V High Grade CA	*The key is resistant to ROCA*
	RENIEC Class VI High Grade CA	*The key is resistant to ROCA*
	RENIEC High Grade Time-Stamping Authority	*The key is resistant to ROCA*

Impacto en los CD emitidos por el RENIEC

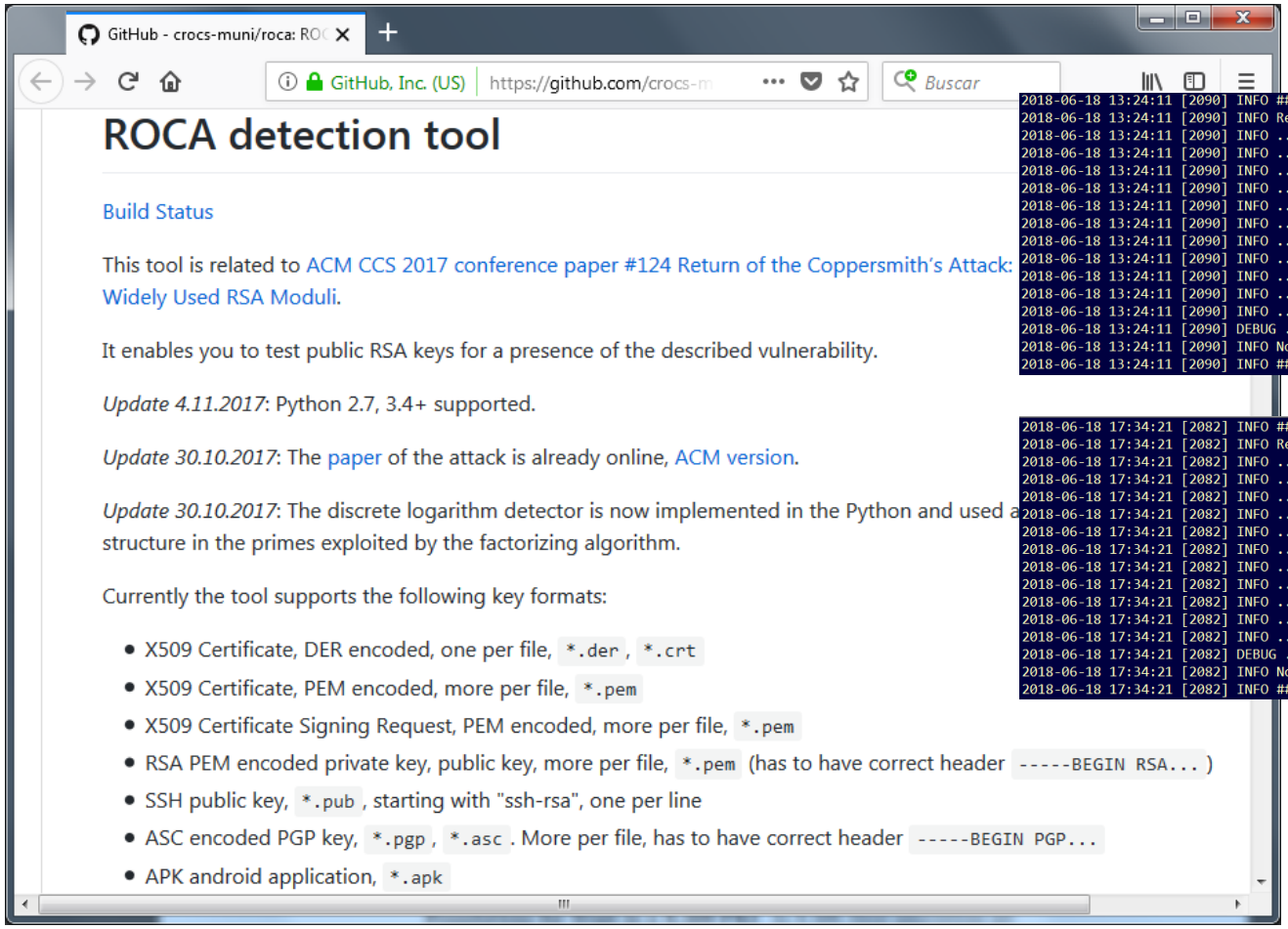
Fase 2: Análisis de los CD de Entidad Final, los cuales cuentan con llaves RSA de 2048 bits

```
2018-06-18 13:24:11 [2090] INFO ### SUMMARY ####################
2018-06-18 13:24:11 [2090] INFO Records tested: 670508
2018-06-18 13:24:11 [2090] INFO .. PEM certs: . . . 670508
2018-06-18 13:24:11 [2090] INFO .. DER certs: . . . 0
2018-06-18 13:24:11 [2090] INFO .. RSA key files: . 0
2018-06-18 13:24:11 [2090] INFO .. PGP master keys: 0
2018-06-18 13:24:11 [2090] INFO .. PGP total keys:  0
2018-06-18 13:24:11 [2090] INFO .. SSH keys:  . . . 0
2018-06-18 13:24:11 [2090] INFO .. APK keys:  . . . 0
2018-06-18 13:24:11 [2090] INFO .. JSON keys: . . . 0
2018-06-18 13:24:11 [2090] INFO .. LDIFF certs: . . 0
2018-06-18 13:24:11 [2090] INFO .. JKS certs: . . . 0
2018-06-18 13:24:11 [2090] INFO .. PKCS7: . . . . . 0
2018-06-18 13:24:11 [2090] DEBUG . Total RSA keys . 670508  (# of keys RSA extracted & analyzed)
2018-06-18 13:24:11 [2090] INFO No fingerprinted keys found (OK)
2018-06-18 13:24:11 [2090] INFO ################################
```

```
2018-06-18 17:34:21 [2082] INFO ### SUMMARY ####################
2018-06-18 17:34:21 [2082] INFO Records tested: 858133
2018-06-18 17:34:21 [2082] INFO .. PEM certs: . . . 858133
2018-06-18 17:34:21 [2082] INFO .. DER certs: . . . 0
2018-06-18 17:34:21 [2082] INFO .. RSA key files: . 0
2018-06-18 17:34:21 [2082] INFO .. PGP master keys: 0
2018-06-18 17:34:21 [2082] INFO .. PGP total keys:  0
2018-06-18 17:34:21 [2082] INFO .. SSH keys:  . . . 0
2018-06-18 17:34:21 [2082] INFO .. APK keys:  . . . 0
2018-06-18 17:34:21 [2082] INFO .. JSON keys: . . . 0
2018-06-18 17:34:21 [2082] INFO .. LDIFF certs: . . 0
2018-06-18 17:34:21 [2082] INFO .. JKS certs: . . . 0
2018-06-18 17:34:21 [2082] INFO .. PKCS7: . . . . . 0
2018-06-18 17:34:21 [2082] DEBUG . Total RSA keys . 858133  (# of keys RSA extracted & analyzed)
2018-06-18 17:34:21 [2082] INFO No fingerprinted keys found (OK)
2018-06-18 17:34:21 [2082] INFO ################################
```

Impacto en los CD emitidos por el RENIEC

Fase 2: Análisis de los CD de Entidad Final, los cuales cuentan con llaves RSA de 2048 bits




```
2018-06-18 13:24:11 [2090] INFO ### SUMMARY ###################
2018-06-18 13:24:11 [2090] INFO Records tested: 670508
2018-06-18 13:24:11 [2090] INFO .. PEM certs: . . . 670508
2018-06-18 13:24:11 [2090] INFO .. DER certs: . . . 0
2018-06-18 13:24:11 [2090] INFO .. RSA key files: . 0
2018-06-18 13:24:11 [2090] INFO .. PGP master keys: 0
2018-06-18 13:24:11 [2090] INFO .. PGP total keys:  0
2018-06-18 13:24:11 [2090] INFO .. SSH keys:  . . . 0
2018-06-18 13:24:11 [2090] INFO .. APK keys:  . . . 0
2018-06-18 13:24:11 [2090] INFO .. JSON keys: . . . 0
2018-06-18 13:24:11 [2090] INFO .. LDIFF certs: . . 0
2018-06-18 13:24:11 [2090] INFO .. JKS certs: . . . 0
2018-06-18 13:24:11 [2090] INFO .. PKCS7: . . . . . 0
2018-06-18 13:24:11 [2090] DEBUG . Total RSA keys . 670508  (# of keys RSA extracted & analyzed)
2018-06-18 13:24:11 [2090] INFO No fingerprinted keys found (OK)
2018-06-18 13:24:11 [2090] INFO ################################
```

```
2018-06-18 17:34:21 [2082] INFO ### SUMMARY ###################
2018-06-18 17:34:21 [2082] INFO Records tested: 858133
2018-06-18 17:34:21 [2082] INFO .. PEM certs: . . . 858133
2018-06-18 17:34:21 [2082] INFO .. DER certs: . . . 0
2018-06-18 17:34:21 [2082] INFO .. RSA key files: . 0
2018-06-18 17:34:21 [2082] INFO .. PGP master keys: 0
2018-06-18 17:34:21 [2082] INFO .. PGP total keys:  0
2018-06-18 17:34:21 [2082] INFO .. SSH keys:  . . . 0
2018-06-18 17:34:21 [2082] INFO .. APK keys:  . . . 0
2018-06-18 17:34:21 [2082] INFO .. JSON keys: . . . 0
2018-06-18 17:34:21 [2082] INFO .. LDIFF certs: . . 0
2018-06-18 17:34:21 [2082] INFO .. JKS certs: . . . 0
2018-06-18 17:34:21 [2082] INFO .. PKCS7: . . . . . 0
2018-06-18 17:34:21 [2082] DEBUG . Total RSA keys . 858133  (# of keys RSA extracted & analyzed)
2018-06-18 17:34:21 [2082] INFO No fingerprinted keys found (OK)
2018-06-18 17:34:21 [2082] INFO ################################
```

https://github.com/crocs-muni/roca

Conclusiones

- Utilizando las herramientas publicadas por los investigadores del CROCS se han verificado 1’528,657 de certificados digitales de Entidad

- La vulnerabilidad ROCA hace posible, con relativamente poco esfuerzo, la factorización de las llaves públicas RSA que fueron generadas bajo dos condiciones:
  - utilizando un chip de la compañia *Infineon Technologies AG* y
  - utilizando la library “RSALib versión 1.02.013”.
- De acuerdo a la Autoridad de los Sistemas de Información de Estonia (ISA, 2018) son once (11) los países en el mundo cuyos documentos de identidad electrónicos (DNIe) son vulnerables al ataque ROCA: **Estonia, España, Eslovaquia, Austria, Polonia, Bulgaria, Kosovo, Italia, Taiwan, Brasil y Malasia.**

sentido que ninguno de los certificados digitales verificados (emitidos por el RENIEC) contiene llaves públicas RSA vulnerables al ataque ROCA.

Bibliografía

- M. Nemec, M. Sys, P. Svenda, D. Klinec and V. Matyas. *The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli*. 24th ACM Conference on Computer and Communications Security (CCS'2017). 1631-1648. 2017. ACM.
  - Conference slides: https://crocs.fi.muni.cz/_media/public/papers/ccs-nemec-handout.pdf
  - Conference paper: https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf
- Information System Authority (ISA), Republic of Estonia. *ROCA Vulnerability and eID: Lessons Learned*. 2018. Disponible en https://www.ria.ee/public/PKI/ROCA-Vulnerability-and-eID-Lessons-Learned.pdf
- Computer Emergency Response Team - European Union (CERT-EU), 2017. *RSA Key Generation Prone to Factorization Attack*. CERT-EU Security Advisory 2017-023. Nov., 2017 — v1.1. Disponible en http://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-023.pdf

Gracias

Impacto del ataque *ROCA** en los certificados digitales emitidos por el RENIEC

Alvaro Cuno
Gerencia de Registros de Certificación Digital
21 de Agosto de 2018

[*ROCA = *The Return of Coppersmith Attack*]