II Taller de criptografía aplicada

Historia: ¿Existió Camazón?

Francisco J.  (Tsao) Santín
e-mail: tsao en linuxbeat punto net
Grupo de Programadores y Usuarios de Linux- Coruña Linux Users Group
GPUL-CLUG

15 de Marzo de 2005

Enigma (I)

Estado del arte en criptografía en la década 1930-40: Algoritmos de sustitución:

- Monoalfabéticos: algortimo de César,ROT13
- Homofónicos:Duque de Mantua (1401)
- "Poligram"?:Playfair (I Guerra Mundial)
- Polialfabéticos: Leon Battista (1568), cifrado de Vigenère, XOR

Enigma (II)

- Algoritmos de trasposición:ADFGVX (I Guerra Mundial)
- Maquinas de rotor (polialfabético): Enigma (II Guerra Mundial)
- Libretas de uso único:Mayor Joseph Mauborgne (1917)

Enigma(III)

- Esteganografía
- Códigos

Enigma(IV)

Hugo Alexander Koch (Delft, Holanda),1919:Geheimschrijfmachine (maquina de escritura secreta)

Arthur Scherbius(Wilmersdorf-Berlin,Alemania): inventor del rotor, poseedor de la patente de la Geheimschrijfmachine desde 1927. Primeros modelos de Enigma, comerciales

Enigma(V)

¿De que se compone la clave de una máquina Enigma?

- Tipo y orden de los rotores
- Disposición del anillo alrededor de los rotores
- Orientación de los rotores
- Cableado del tablero de conexiones

Enigma(VI)

Maquina Enigma (http://www.cs.usfca.edu/www.AlanTuring.net/ turing_archive/pages/Reference%20Articles/codebreaker.html)

La historia conocida

Bletchley Park(foto de A.Quirantes,

`http://www.ugr.es/~ aquiran/cripto/museo/bp2002/bp.htm)`

La historia conocida(II)

Colussus (reconstrucción, foto de A.Quirantes,

`http://www.ugr.es/~aquiran/cripto/museo/bp2002/bp.htm`)

La historia conocida(III)

Alan Turing

La historia conocida(IV)

Ingleses y franceses consideran indescifrable la Enigma militar hasta los años 30

Sin embargo, Hugh Foss a finales de los 20 ataca con éxito versiones comerciales (método "rodding"); Dilly Knox mejora el procedimiento usando como pruebas los mensajes de la Guerra Civil Española

Se basa en preveer información sobre el mensaje y en el funcionamiento de los rotores de Enigma

En España...(I)

A día de hoy, cualquier documento relacionado con criptografía del Estado es materia clasificada

Dos autores destacables: Arturo Quirantes y Josep Ramon Soler

En España...(II)

Principales métodos "manuales" usados en la Guerra Civil:

- Códigos (códigos de trinchera):facilidad de uso,¿de reemplazo? , reducción de mensaje,inflexibilidad: clave de bous, marina republicana

- Códigos de guerrilla: esteganografía de código: Agrupación Guerrillera de Levante

- Métodos de sustitución y/o transposición: Clave X (republicana, Mar Cantábrico), la clave Fenicia y la clave de la XIV División (nacional)

En España...(III)

- Criptógrafo de cinta (sustitución múltiple): los más usados por ambos bandos

- Cifrados de rejilla (usados por primera vez por el matemático Girolamo Cardano en el siglo XVI)

En España...(IV)

Principales máquinas usadas en los años 30 y Guerra Civil:

Kryha:

- alemana
- el gobierno se decanta por ella en 1931 en detrimento de Enigma por motivos publicitarios
- en 1933 William Friedman (americano) descifra un mensaje en 2 horas y 41 minutos

En España...(V)

- en el mismo 1933 el gobierno encarga dos, y mas tarde una a mayores (2700 marcos de *fondos reservados*)

En España...(VI)

Wheatstone:

- Dos ruedas, una con alfabeto en claro y otro cifrado, bloques de 4 letras
- Nace en USA en el siglo XIX, descartada en general después de la I WW
- Conocida en España como clave Norte/clave San Carlos

En España...(VII)

- Usada en las comunicaciones desde 1937, para comunicaciones entre el alto mando nacional, el Ejército Norte, el Cuerpo de Ejército, 5^a, 6^a y 8^a divisiones, las Divisiones Ávila y Soria, y el Ejército Sur.

- Conocemos de su existencia gracias al espionaje británico

En España...(VIII)

Enigma:

- El bando nacional recibe como ayuda de Alemania un modelo comercial de Enigma (K), aunque hasta ahora sólo se ha confirmado que la utilizaron los alemanes de la Legión Condor y los italianos en nuestra guerra

- El 24 de abril de 1937 el criptoanalista británico Dilly Knox logra descifrar un mensaje transmitido entre las fuerzas del bando nacional

En España...(IX)

- Después de la Guerra Civil, un número indeterminado de Enigmas se quedaron en España (al menos 15)y se siguieron usando hasta los años 50, recableadas

- Método de distribución de claves irrisorio

- Uso durante la II WW entre Madrid y Berlín, ayudando a BP

Polonia, la gran olvidada (I)

Polonia realiza una intensa actividad criptoanalítica en los años 30, en previsión de una invasión por parte de Alemania

Intercambia información técnica con británicos y franceses

Polonia, la gran olvidada (II)

1939-Alemania invade Polonia

¡Sorpresa! Marian Rejewski, Jerzy Rozycki y Henryk Zygalski hacía años que habían criptoanalizado la versión militar de Enigma y habían construído dispositivos ("bombas") que permitían mecanizar parte del proceso de criptoanálisis. Soluciones matemáticas e información sobre el manejo de claves permiten la reconstrucción de la máquina: método de las huellas (antes de 1938), método de la bomba polaca

Los tres escapan a Francia, y trabajan entre Argelia (puesto Kouba) y Francia (puesto Cadix). Rozycki muere en enero del 42

Después de la invasión de Francia, huyen a Inglaterra via España, Portugal y Gibraltar

En Gran Bretaña son marginados "por ser sospechosos"

El equipo D

Tras acabar la guerra civil, viajan entre los refugiados a Francia, un grupo de cinco criptoanalistas que trabajaron durante la guerra en Barcelona. Sólo se conoce el apellido de uno (y de forma dudosa).

Fueron encontrados ¿? por el que a la postre se convirtió en el jefe del servicio de criptoanálisis francés, Gustave Bertrand y enrolados junto con dos comisarios políticos republicanos bajo nombre falso en la Legión Extranjera

El llamado Equipo D se unió a otros grupos de criptoanalistas extranjeros, incluyendo el Equipo Z de Rejewski y otros 50 franceses, se establece el puesto Bruno en el castillo de Vignoles, cerca de Gretz-Armanvilliers

El equipo D (II)

En 1940 con la invasión de Paris el puesto Bruno es trasladado a Argelia, luego a la Francia no ocupada

Criptoanalistas polacos y españoles en el centro Cadix (Sur de Francia, 1942)

De izquierda a derecha: 1 - Marian Rejewski; 2 - Edward Fokczynski; 3 - español no identificado; 4 - Henryk Zygalski 5 - español no identificado; 6 - Jerzy Rozycki; 7 - español no identificado; 8 - Antoni Palluth; 9 - español no identificado.

(http://www.ugr.es/~aquiran/cripto/museo.htm)

Bibliografía

- "Applied cryptography", de Bruce Schneier.Wiley & Sons, 2ª ed.1996

- "Boletin Enigma", de Arturo Quirantes (ver Direcciones de interés)

- "Seizing the Enigma: Race to Break the German U-boat Codes, 1939-43", de David Kahn. Arrow, 1996

- "Apunts de Criptologia I historia", de Josep Ramon Soler Fuensanta

Bibliografía (II)

- "The Codebreakers",de David Kahn. Scribner,1996

- "Criptonomicón", de Neal Stephenson.Ediciones B,2004 ;-)

Direcciones de interés

- Página de homenaje a Alan Turing:

  `http://www.alanturing.net`

Direcciones de interés (II)

- Página sobre la Guerra Civil Española en Euskadi:

  `http://es.geocities.com/gce_euzkadi/paginas/cifra.html`

- Taller de criptografía de Arturo Quirantes:

  `http://www.ugr.es/~aquiran/cripto/cripto.htm`

- Kriptópolis:http://www.kriptopolis.org/enigma

Cine

- Enigma (Michael Apted, 2001): muy detallista, en los procedimientos para el manejo de la máquina Enigma. Recomendable

- Das Boot (El Submarino) (Wolfgang Petersen, 1981):muy bien ambientada, probablemente la mejor película de submarinos de la historia

- U-571 (Jonathan Mostow,2000): para comer con palomitas... y antiácidos, probablemente la peor película de submarinos de la historia

- The enemy below (Duelo en el Atlántico)(Dirk Powell,1957) : no recuerdo bien si sale una Enigma (creo que si), pero es probablemente la segunda mejor película de submarinos de la historia :-D