Churchill's ULTRA Secret of the Century

ULTRA = Codename für allen Erkenntnis-gewinn durch Entziffern deutscher, italienischer, japanischer kodierter Nachrichten.

12 000 Männer und Frauen der GCCS in Bletchley Park hatten durch Eid auf den König und das Land geschworen noch 3 Jahrzente nach dem Krieg weder über ihre Arbeit zu reden noch zu schreiben.

Dieses Schweigen wurde beendet durch das Buch "The ULTRA Secret" von Capitain Winterbloom in 1974. Die von Winterbloom veröffentlichten Fakten waren damit nicht mehr geheim.

Winston Churchill erwähnte Bletchley Park mit keinem Wort auch nicht in dem 6-Völker Buch über Word WAR II publiziert in 1948-1953. Tausende von Bücher von Generälen, Admirälen, und zivilen nicht militärischen Führern schweigen komplett über GCCS und Bletchly Park

Churchill war zu vielen Anlässen während des Krieges in Bletchly Park. Er bezeichnete die Arbeiter dort als

"the geese that laid golden eggs but never cackled".

Churchill sprach selbst mit der führenden Kryptographen darunter A. Turing im Sept 1941 um ihre Moral anzuspornen.
A. Turing's Gruppe von mathematischen Cracks schrieb im Okt. 1941 persönlich an Churchill, unter Umgehung ihrer Vorgesetzten mit der Bitte um mehr Personal für ihre Gruppe. Churchill reagierte umgehend mit einem Memorandum an den principal staff officer:
"Make sure they have all they want on extreme priority and report to me that this has been done"
Das Resultat: Der Rechensaal von etwa 50 decodierten Fachkräften die Woche im 1940 wuchs zu einer Flut von 3000 am Tag im 1943

Die ursprünglich Zahnrad getriebenen "Bomben" wurden durch neu erfundene revolutionäre elektronische, programmierbare Computer ersetzt. Code name: Colossus. Die eigentliche Aufgabe der größten Colossus mit 2.500 Röhren war es die persönlichen Anweisungen von Hitler an seine Führenden Generäle zu lesen und zu decodieren. Hitlers Anweisungen wurden mit dem Lorenz 12 rotor cipher Geheimschreibmaschine (eine Weiterentwicklung der ENIGMA) Bletchley P. knackte Enigma Post vollständig entschlüsseln Stunden bevor sie von deutschen

Befehlsketten wie Goering, Guderian oder Rommel gelesen wurden.
Churchill las beim Frühstück in London dieselbe Post die Hitler erst gegen Abend bekam.

Colossus in Bletchley Park war der weltweit erste elektronische Rechner. Er war mit fast 10 Jahre vor der ENIAC in USA im Betrieb. Die Existenz von Colossus war geheim bis 1975. Colossus war mit sehr effizienten Schreibmaschinen zur Ein- und Ausgabe ausgestattet. 5.000 characters per second, tape 30 miles per hour.

Nach Kriegsende ordnete Churchill ~~die~~ an, alle Code brechende Maschinen in Stücke nicht größer als eine Hand zu zertrümmern.

10 Colossus Maschinen und 150 mechanische "Bomben" wurden so zerstört. Die Bedeutung der Kryptographie für die Kriegsführung sollte geheim bleiben.

Im Krieg erbeutete man ENIGMA Maschinen dadurch, dass man deutsche Wetterschiffe versenkte. Nach dem Krieg verkaufte man Tausende der erbeuteten ENIGMA Maschinen an die Kolonien, die glaubten dass diese Codierung noch sicher war.

Bletchley Park

Die Government Code and Cypher School (GCCS) zog 1939 in das Mansion von Bletchley Park, im Dreieck von London, Oxford und Cambridge

Direkt Zugverbindung nach London, Oxford und Cambridge, schneller Zugang für Kuriere, Messerschaffer.
Bletchley Park ist nahe zu einem zentralen Punkt des Telecommunication Netzwerkes mit Kommunikations-Linien hoher Kapazität. Abgeschiedener Platz, nicht abzuschirmen, keine Bebauung oder Menschen in der Nähe.

(Selbst Marian Rejewski ein Mathematiker des Polnischen Cipher Bureaus, der eine erste Version der ENIGMA analysierte und nach Frankreich nach England geflüchtet war arbeitet für die GCCS aber ohne Zugang nach Bletchley Park.
Ab Sept 1936 bekam die GCCS erstmals eine Gruppe von Mathematikern als Codebrecher, zu der dann A. Turing stieß. Diese Mathematiker Gruppe in Hütte 8 baute auf dem Wissen der Mathematiker des Polnischen Cypher Büros auf. (Hut 8 unter der Leitung von A. Turing und ab Okt. 1941 zeitweise Stellvertreter H. Alexander arbeitete an der Entzifferung der Funksprüche der Marine welche ENIGMA-M3 und ENIGMA-M4

Alan Turing 1912–1954

Alan und sein älterer Bruder John werden von einem Armee-Ehepaar im Rheinland in England groß gezogen während Vater und Mutter in Indien im Zivildienst tätig waren.

King's College Cambridge 1931–1934

Fellow des King's College 1935 aufgrund seiner Dissertation.

1937: Grundlegendes Paper

"On computable Numbers with Application to the Entscheidungsproblem"

Entscheidungsproblem of David Hilbert

Turing gab eine neue Darstellung zu Kurt Gödel 1931 Resultaten zur Grenze von Beweisbarkeit und Berechenbarkeit. Turing ersetzt Kurt Gödel universelle arithmetik-basierte formale Sprache durch ein formales, einfaches Rechenkonzept, das als Turing machine bekannt wurde. Turing bewies, dass das Hilbertproblem für diese Maschinen nicht entscheidbar ist. Turing's Ansatz ist viel besser zugänglich als die früheren Ansätze von Gödel und Church (Lambda calculus)

Seit 1938/39 arbeitet Turing für die

GCCS an der Kryptanalyse der ENIGMA.

Besondere Beiträge

Turing verallgemeinert die Analyse von M. Rejewski zu einem stabilen Ansatz.

Turing nutzt statistische Analyse um die verschiedenen Möglichkeiten beim Code-brechen zu optimieren.

Papers: Report on the application of probability to Cryptography

Paper on statistics of repetitions

Aufgrund der Bedeutung dieser Arbeiten für die GCCS und die spätere GCHQ wurden die Arbeiten erst im April 2012 dem UK National Archive freigegeben, anlässlich des 100-sten Geburtstages von Turing.

1982 – 1994: Crypto AG

Falklandkrieg: Die USA unterstützten Großbritannien u.a. durch Entschlüsselung des Funkverkehrs der argentinischen Streitkräfte

1986: Präsident Reagan erhält davon Beweise, daß Muhammar El Gaddafi die Bomben in der Berliner Diskothek angeordnet hat (Abhören des Funkverkehrs Tripoli – Konsulat von Lybien in Berlin)

Lockerbie Attentat, Pan Am Flug 103, 21. Dez. 1988

1991, 6. April: Ermordung von Schapur Bakhtiar (ehemaliger iranischer Ministerpräsident) in Paris. Der verschlüsselte Funkverkehr der iranischen Botschaft in Paris wurde von der CIA der Presse zugespielt und veröffentlicht (in Le Monde)

Argentinien, Iran und Lybien benutzten Verschlüsselungen der CRYPTO AG, Steinhausen Schweiz.

Hans Bühler der Verkaufsverkehr der CRYPTO AG in Teheran wurde am 18. März 1992 in Teheran verhaftet und nach 9 Monaten gegen ein Lösegeld von 1 Million US $, gezahlt von der Crypto AG, freigelassen. Bühler wurde nach Rückkehr in die Schweiz vorgehalten von der Crypto AG entlassen und zur Rückzahlung des Lösegeldes angehalten.

11. Bühler im Radio Interview:
There are several people at Crypto AG who knew about manipulating machines since 1970 and even before. Die Crypto AG hatte engen Kontakt und häufig Besuch vom BND und der NSA.

NSA, Fort Meade Maryland

etwa 38.000 Mitarbeiter geschätzt, darunter 7.000 Mathematiker. Weltweit größter Arbeitgeber für Mathematiker.

DSA, El-Gamal und Schnorr Signatur

Diese Signaturen beruhen auf dem Diskreten Logarithmus.

Die Schnorr Signatur wurde 1990 / 1991 veröffentlicht mit Sicherheitsbeweis.
Abstract Eurocrypt 1989 Houthalen Belgien
Krafzig (NSA) war bei dem Vortrag in der Rump session.

Die Schnorr Signatur wurde zunächst intern von der NSA zum DSA ausgewählt, musste aber dann, weil sie patentiert war, abgeändert werden.

DSA: Variante von Elgamal und Schnorr Signatur
Bei der Variante geht der Sicherheitsbeweis verloren.
FIPS Pub 186-1 (1992)

Serge Vaudenay CRYPTO 1996 pp 83→87
Hidden Collisions on DSS.

Warum wählt die NSA
DSA eine Variante der Schnorr Signatur
und nicht RSA ?

DSA ist wie die Schnorr Signatur nur zum
Signieren verwendbar und nicht zum Kodieren.

RSA ist zum chiffrieren (kodieren) und
signieren verwendbar.
Die RSA-Kodierung schützt die
Informationsübertragung im Internet.

RSA kooperiert nicht mit der NSA
etwa in der Art wie die CRYPTO AG.

Die NSA hatte ein Interesse daran RSA
abzudrängen

Aufgrund meines Lizenzvertrags zur Schnorr
Signatur mit RSA war ich 15 Jahre
Mitglied des Scientific Boards von RSA.

Die wirtschaftliche Bedeutung des Internets
ist inzwischen grösser als die der Verteidigungs-
industrie

Google, Apple, Microsoft
Yahoo

711 Milliarden $
Mc Donnell Douglas
Boeing

Privacy in Information Retrieval

2009-202 Stex net, Flame 2010-212

2012 : Prime collisions in RSA keys

2012 The End of Crypto

What good is e2ee if endpoints aren't secure?