Crypto City und die NSA

Maik Lange und Raffael Dzikowski

Humboldt-Universität zu Berlin
Geschichte der Verschlüsselung

21.11.2006

Index

NSA Entstehung 1 - ASA

- ASA - ArmySecurityAgency - 1945-1977

NSA Entstehung 1 - ASA

- ASA - ArmySecurityAgency - 1945-1977
- Operierte beim US Heer

NSA Entstehung 1 - ASA

- ASA - ArmySecurityAgency - 1945-1977
- Operierte beim US Heer

Ziel

Auffangen von Feindnachrichten und Kryptologie

NSA Entstehung 1 - ASA

- ASA - ArmySecurityAgency - 1945-1977
- Operierte beim US Heer
- ASA ging über zur INSCOM (US Army Intelligence and Security Command)

Ziel

Auffangen von Feindnachrichten und Kryptologie

NSA Entstehung 2 - AFSA

- AFSA - ArmedForcesSecurityAgency - 1949-1951

NSA Entstehung 2 - AFSA

- AFSA - ArmedForcesSecurityAgency - 1949-1951
- Operierte bei Heer, Marine und Luftwaffe

NSA Entstehung 2 - AFSA

- AFSA - ArmedForcesSecurityAgency - 1949-1951
- Operierte bei Heer, Marine und Luftwaffe

Ziel

Kryptologische Tätigkeiten der US Armee vereinen

NSA Entstehung 2 - AFSA

- AFSA - ArmedForcesSecurityAgency - 1949-1951
- Operierte bei Heer, Marine und Luftwaffe
- 1951 wegen Mängeln (in der Fernmeldeaufklärung) von H.S. Truman aufgelößt

Ziel

Kryptologische Tätigkeiten der US Armee vereinen

NSA Entstehung 3 - NSA

- NSA - National Security Agency

NSA Entstehung 3 - NSA

- NSA - National Security Agency
- Harry S. Truman (1945-1953) am 4.10.1952 gegründet

NSA Entstehung 3 - NSA

- NSA - National Security Agency
- Harry S. Truman (1945-1953) am 4.10.1952 gegründet

Ziel

Abhören ausländischer Nachrichten

NSA Entstehung 3 - NSA

- NSA - National Security Agency
- Harry S. Truman (1945-1953) am 4.10.1952 gegründet
- Operiert unabhängig

Ziel

Abhören ausländischer Nachrichten

NSA Direktor

Abbildung: Lt.Gen. Keith Alexander

NSA Daten

- Aktueller Leiter seit 2005 Keith Alexander

NSA Daten

- Aktueller Leiter seit 2005 Keith Alexander
- ca. 38.000 Mitarbeiter

NSA Daten

- Aktueller Leiter seit 2005 Keith Alexander
- ca. 38.000 Mitarbeiter
- NSA Budget 1999 26,6mrd - heute unbekannt

Crypto City

- Hauptquartier der NSA in Fort Meade (Maryland)

Crypto City

- Hauptquartier der NSA in Fort Meade (Maryland)
- nicht in Karten verzeichnet

Crypto City

- Hauptquartier der NSA in Fort Meade (Maryland)
- nicht in Karten verzeichnet
- 4km große Fläche

Crypto City

- Hauptquartier der NSA in Fort Meade (Maryland)
- nicht in Karten verzeichnet
- 4km große Fläche
- umfasst ca. 50 Gebäude

Crypto City

- Hauptquartier der NSA in Fort Meade (Maryland)
- nicht in Karten verzeichnet
- 4km große Fläche
- umfasst ca. 50 Gebäude
- enthält eigene Chipfabrik

Crypto City

- Hauptquartier der NSA in Fort Meade (Maryland)
- nicht in Karten verzeichnet
- 4km große Fläche
- umfasst ca. 50 Gebäude
- enthält eigene Chipfabrik
- Eigene Polizei
  - bewacht von den “Men in Black„
  - Executive Protection Unit stellt Fahrer und Leibwächter

Crypto City aus dem All

Crypto City Hauptgebäude

Abbildung: NSA Hauptgebäude

Aufbau der NSA

In Abteilungen gegliedert

- Central Security Service (CSS)

Aufbau der NSA

In Abteilungen gegliedert

- Central Security Service (CSS)
  - Überwachen Fernmeldeaufklärung

Aufbau der NSA

In Abteilungen gegliedert

- Central Security Service (CSS)
  - Überwachen Fernmeldeaufklärung
- Diretorate of Operations (DO)

Aufbau der NSA

In Abteilungen gegliedert

- Central Security Service (CSS)
  - Überwachen Fernmeldeaufklärung
- Diretorate of Operations (DO)
- Defense Special Missile and Astronautics Center (DEFSMAC)

Aufbau der NSA

In Abteilungen gegliedert

- Central Security Service (CSS)
  - Überwachen Fernmeldeaufklärung
- Diretorate of Operations (DO)
- Defense Special Missile and Astronautics Center (DEFSMAC)
  - überwacht Raketenstarts und Raumfahrt

Generationen der Verschlüsselung

Info

Einteilung der NSA Verschlüsselungsysteme der letzten 50 Jahre

Generationen der Verschlüsselung

Info

Einteilung der NSA Verschlüsselungsysteme der letzten 50 Jahre

Generationen

1. Elektro-Mechanische

Generationen der Verschlüsselung

Info

Einteilung der NSA Verschlüsselungsysteme der letzten 50 Jahre

Generationen

1. Elektro-Mechanische
2. Elektronenröhren

Generationen der Verschlüsselung

Info

Einteilung der NSA Verschlüsselungsysteme der letzten 50 Jahre

Generationen

1. Elektro-Mechanische
2. Elektronenröhren
3. Integriete Schaltkreise

Generationen der Verschlüsselung

Info

Einteilung der NSA Verschlüsselungsysteme der letzten 50 Jahre

Generationen

1. Elektro-Mechanische
2. Elektronenröhren
3. Integriete Schaltkreise
4. Elektronischen Schlüsselverteilung

Generationen der Verschlüsselung

Info

Einteilung der NSA Verschlüsselungsysteme der letzten 50 Jahre

Generationen

1. Elektro-Mechanische
2. Elektronenröhren
3. Integriete Schaltkreise
4. Elektronischen Schlüsselverteilung
5. Netzwerk orientierte Systeme

I Elektro-Mechanische Generation

- ab ca. 1952

I Elektro-Mechanische Generation

- ab ca. 1952
- Weiterentwicklungen von WWII Geräten

I Elektro-Mechanische Generation

- ab ca. 1952
- Weiterentwicklungen von WWII Geräten
- es waren Rotormachinen

I Elektro-Mechanische Generation

- ab ca. 1952
- Weiterentwicklungen von WWII Geräten
- es waren Rotormachinen
- täglich wechselnde Schlüssel (Codebuch)

I Elektro-Mechanische Generation

- ab ca. 1952
- Weiterentwicklungen von WWII Geräten
- es waren Rotormachinen
- täglich wechselnde Schlüssel (Codebuch)

Abbildung: WWII - SIGABA

I Elektro-Mechanische Generation

- ab ca. 1952
- Weiterentwicklungen von WWII Geräten
- es waren Rotormachinen
- täglich wechselnde Schlüssel (Codebuch)

Abbildung: WWII - SIGABA

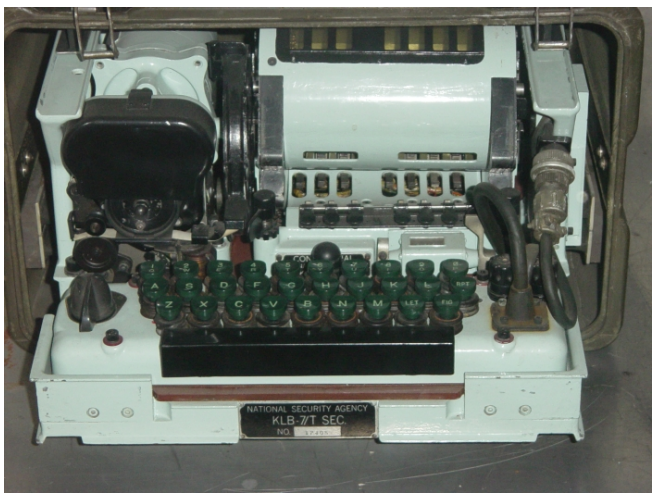


Abbildung: NSA´s - KL7

I Elektro-Mechanische Generation

- ab ca. 1952
- Weiterentwicklungen von WWII Geräten
- es waren Rotormachinen
- täglich wechselnde Schlüssel (Codebuch)
- KL7 bis 1983 in gebrauch

Abbildung: WWII - SIGABA

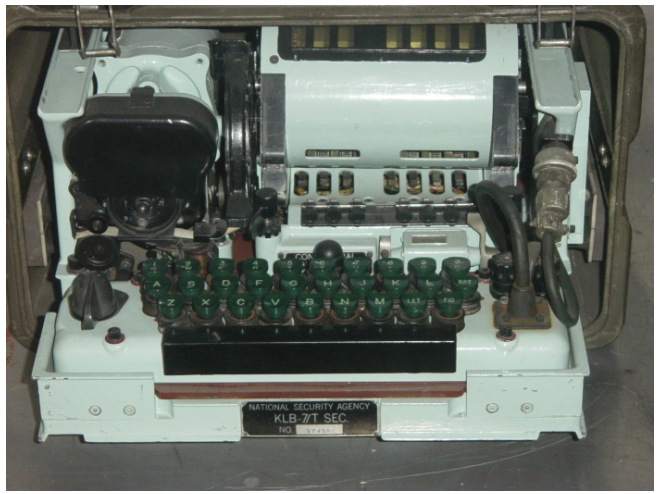


Abbildung: NSA´s - KL7

II Elektronenröhren Generation

- ab 1970

II Elektronenröhren Generation

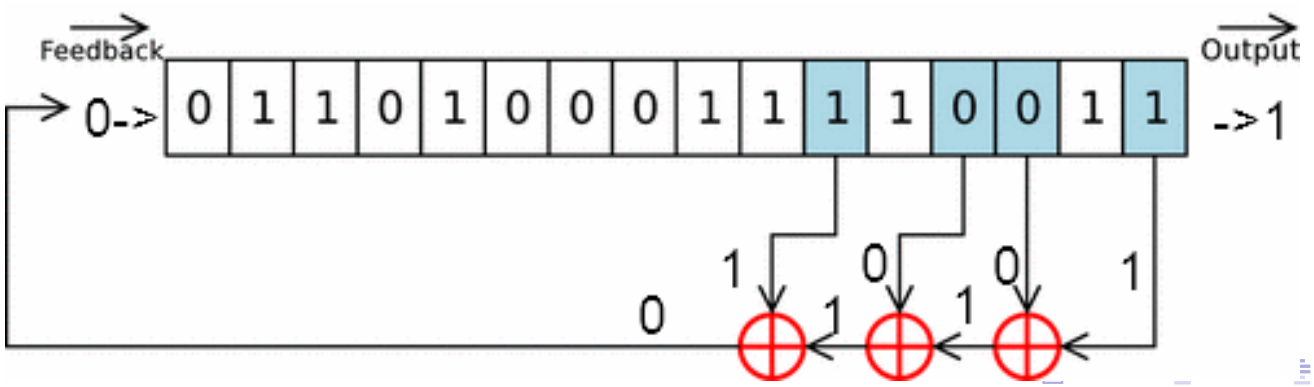
- ab 1970
- bestanden aus Elektronenröhren

II Elektronenröhren Generation

- ab 1970
- bestanden aus Elektronenröhren
- Algorithmen basierten auf linear rückgekoppelten Schieberegistern

II Elektronenröhren Generation

- ab 1970
- bestanden aus Elektronenröhren
- Algorithmen basierten auf linear rückgekoppelten Schieberegistern



II Elektronenröhren Generation

- ab 1970
- bestanden aus Elektronenröhren
- Algorithmen basierten auf linear rückgekoppelten Schieberegistern
- Schlüssel auf Lochkarten
- täglich wechselnde Schlüssel

II Elektronenröhren Generation

- ab 1970
- bestanden aus Elektronenröhren
- Algorithmen basierten auf linear rückgekoppelten Schieberegistern
- Schlüssel auf Lochkarten
- täglich wechselnde Schlüssel
- mußten häufig gewartet werden

II Elektronenröhren Generation

- ab 1970
- bestanden aus Elektronenröhren
- Algorithmen basierten auf linear rückgekoppelten Schieberegistern
- Schlüssel auf Lochkarten
- täglich wechselnde Schlüssel
- mußten häufig gewartet werden
- warem unempfindlich gegenüber EMP´s

II Elektronenröhren Generation

- ab 1970
- bestanden aus Elektronenröhren
- Algorithmen basierten auf linear rückgekoppelten Schieberegistern
- Schlüssel auf Lochkarten
- täglich wechselnde Schlüssel
- mußten häufig gewartet werden
- warem unempfindlich gegenüber EMP´s
- bis ca. 1980 in betrieb

III Generation der Integrieten Schaltkreise

- ab 1980
- Transitoren und Schaltkreis basiert mit stärkeren Algorithmen

III Generation der Integrieten Schaltkreise

- ab 1980
- Transitoren und Schaltkreis basiert mit stärkeren Algorithmen
- kleiner und verläßlicher als bisherige Systeme

III Generation der Integrieten Schaltkreise

- ab 1980
- Transitoren und Schaltkreis basiert mit stärkeren Algorithmen
- kleiner und verläßlicher als bisherige Systeme
- Aufrechterhaltung austausch defekter Chips

III Generation der Integrieten Schaltkreise

- ab 1980
- Transitoren und Schaltkreis basiert mit stärkeren Algorithmen
- kleiner und verläßlicher als bisherige Systeme
- Aufrechterhaltung austausch defekter Chips
- Schlüsseleingabe per Lochpapierrolle und entsprechendem Lesegerät

III Generation der Integrieten Schaltkreise 2

Abbildung: Paper Tape

III Generation der Integrieten Schaltkreise 2

Abbildung: Paper Tape

Abbildung: Paper Tape Lesegerät KOI-18

IV Generation der Elektronischen Schlüsselverteilung

- ab 1990

IV Generation der Elektronischen Schlüsselverteilung

- ab 1990
- abwärtskompatibilität zu Systemen der 3ten Generation

IV Generation der Elektronischen Schlüsselverteilung

- ab 1990
- abwärtskompatibilität zu Systemen der 3ten Generation
- Schlüsselgültigkeit war lang (1 Jahr und mehr)

IV Generation der Elektronischen Schlüsselverteilung

- ab 1990
- abwärtskompatibilität zu Systemen der 3ten Generation
- Schlüsselgültigkeit war lang (1 Jahr und mehr)
- Schlüssel lagen als „Security tokens“ oder elektronisch vor

Security Tokens

Abbildung: Security Tokens

IV Generation - Geheime Netzwerke

- erstmals wurde die Verschlüsslung bei Industriellen Standards unterstützt

IV Generation - Geheime Netzwerke

- erstmals wurde die Verschlüsslung bei Industriellen Standards unterstützt
- wie Ethernet oder Internet Protokoll (IP)

IV Generation - Geheime Netzwerke

- erstmals wurde die Verschlüsslung bei Industriellen Standards unterstützt
- wie Ethernet oder Internet Protokoll (IP)
- Bildung geheimer Netzwerke auf Grundlage von Kommerzieller Internet Technologie

IV Generation - Geheime Netzwerke

- erstmals wurde die Verschlüsslung bei Industriellen Standards unterstützt
- wie Ethernet oder Internet Protokoll (IP)
- Bildung geheimer Netzwerke auf Grundlage von Kommerzieller Internet Technologie
- Geheimne Netzwerke wie SIPRNet oder JWICS

IV Generation - Geheime Netzwerke

- erstmals wurde die Verschlüsslung bei Industriellen Standards unterstützt
- wie Ethernet oder Internet Protokoll (IP)
- Bildung geheimer Netzwerke auf Grundlage von Kommerzieller Internet Technologie
- Geheimne Netzwerke wie SIPRNet oder JWICS
- Netzwerke stellten sichere Kommunikation zur verfügung

V Generation der Netzwerk orientierten Systeme

- ab ca. 1995

V Generation der Netzwerk orientierten Systeme

- ab ca. 1995
- NSA unterstützt kommerzielle Firmen beim erstellen Sicherer Systeme für die Regierung

V Generation der Netzwerk orientierten Systeme

- ab ca. 1995
- NSA unterstützt kommerzielle Firmen beim erstellen Sicherer Systeme für die Regierung
- NSA entwickelt sichere Standards wie

V Generation der Netzwerk orientierten Systeme

- ab ca. 1995
- NSA unterstützt kommerzielle Firmen beim erstellen Sicherer Systeme für die Regierung
- NSA entwickelt sichere Standards wie
- Future Narrow Band Digital Terminal (FNBDT)
  - für Sichere Telefonverbindungen

V Generation der Netzwerk orientierten Systeme

- ab ca. 1995
- NSA unterstützt kommerzielle Firmen beim erstellen Sicherer Systeme für die Regierung
- NSA entwickelt sichere Standards wie
- Future Narrow Band Digital Terminal (FNBDT)
  - für Sichere Telefonverbindungen
- High Assurance Internet Protocol Interoperability Standard (HAIPIS)
  - Sichere Datenübertragung über Offene Netzwerke

V Generation der Netzwerk orientierten Systeme

- ab ca. 1995
- NSA unterstützt kommerzielle Firmen beim erstellen Sicherer Systeme für die Regierung
- NSA entwickelt sichere Standards wie
- Future Narrow Band Digital Terminal (FNBDT)
  - für Sichere Telefonverbindungen
- High Assurance Internet Protocol Interoperability Standard (HAIPIS)
  - Sichere Datenübertragung über Offene Netzwerke
  - HAIPE (High Assurance Internet Protocol Encryptor)
  - ist ein Gateway zwischen 2 Sicheren Endpunkten über ein Offenes Netzwerk (zB. Internet)

V Generation der Netzwerk orientierten Systeme 2

Mitentwicklung an Öffentlichen Systemen

- Suite B
- AES
- SHA
- Digital Signature Algorithm
- Security-Enhanced Linux

Generationen Übersicht 1

Nutzungsdauer von Systemen

- Anfangs 30 Jahre (1 Gen.)
- verringert sich Pro Generation um ca 10 Jahre bis zur 4 Gen.
- Verkürzung der Nutzungsdauer bei modernen Systemem

Generationen Übersicht 1

Nutzungsdauer von Systemen

- Anfangs 30 Jahre (1 Gen.)
- verringert sich Pro Generation um ca 10 Jahre bis zur 4 Gen.
- Verkürzung der Nutzungsdauer bei modernen Systemem

Gültigkeitsdauer der Schlüssel

- 1-3 Generation täglicher Schlüsselwechsel (Codebuch)
- 4-5 Generation Jährlich und länger

Generationen Übersicht 2

Schlüsselart

- Anfangs Mechanische Einstellung (Walzen auswahl usw)
- Lochbänder (Paper Tapes) (2 und 3 Generationen)
- Security Tokens, Passwörter (4 und 5 Generation)

Generationen Übersicht 2

Schlüsselart

- Anfangs Mechanische Einstellung (Walzen auswahl usw)
- Lochbänder (Paper Tapes) (2 und 3 Generationen)
- Security Tokens, Passwörter (4 und 5 Generation)

Verteilungsgrad

- zu Beginn bei den Streitkräften
- später als „Dienstleister “ wurden Systeme an Firmen weitergegeben die mit der Regierung zu tun hatten
- Publizierung von Verschlüsselungssysteme für die Öffentlichkeit

Allgemeines

Notwendigkeit

- Kriegsdoktrien der USA erforderte schnelle Kommunikation
- Überbrückung großer Entfernungen

Arten der Verschlüsselung

- Analoge Sprachverschlüsselung
- Digitale Sprachverschlüsselung

Zeitlinie

SIGSALY

STU-III

STE

Echelon

Was ist Echelon?

Weltweites Abhörsystem der Telefon- und Internetkommunikation

Echelon

Was ist Echelon?

Weltweites Abhörsystem der Telefon- und Internetkommunikation

Wer hat daran Teil?

USA, UK, Kanada, Australien und Neuseeland

Echelon

Was ist Echelon?

Weltweites Abhörsystem der Telefon- und Internetkommunikation

Wer hat daran Teil?

USA, UK, Kanada, Australien und Neuseeland

Eckdaten

- unterliegt der NSA Verwaltung
- umfasst 120 Stationen und Satelliten
- ca. 90% des Internetverkehrs wird durchsucht

Bestandteile

Netzwerk-Übersicht

Nutzung von Echelon

- allg. Fernmeldeaufklärung
- Feindverfolgung
- Industriespionage