Die Geschichte der Kryptographie und Kryptoanalysis
ein geschichtlicher Abriß

Bilder zum Vortrag

Steganographie

- Verstecken einer Nachricht.
- Beispiele
  - alte China: auf Seide geschriebene, als Wachsbällchen geschluckte Nachrichten
  - 5 JhvCh: Überraschungsangriff der Perser (Xerxes) auf Athen.
    Warnung von Griechem aus dem Exil auf Holz einer Wachstafel
    Empfänger verwundert über leere Tafel => findet Nachricht
    Athen bereitet sich vor, Persien verliert.
  - Kohlenstoffhaltige Flüssigkeiten als unsichtbare Tinte
    Spione des 20Jhd setzen ihren Urin ein.
  - 2. WW: Mikropunkte: fotographische Verkleinerung => verstecken als i-Punkte einer dummy-Message.
  - verstecken einer Nachricht in niedrigsten Bits einer Wav-Datei verschwimmt im statistischen Rauschen.
- Vorteile:
  - sehr viele Möglichkeiten, Nachrichten zu verstecken.
  - schnelle Improvisation möglich.
- Nachteile:
  - einziger Schutz ist Geheimhaltung der Aktion.
  - zufällige Entdeckung möglich.
  - nicht für den Einsatz im großen Stil geeignet.

Transposition

- unkenntlich machen einer Nachricht durch vertauschen der Reihenfolge der Buchstaben.
- Beispiele
  - Skytale: erstes militärische Krypto-Verfahren.
  - Gartenzaun: Text reihenweise in Tabelle schreiben und spaltenweise auslesen.
- Nachteil: unsicher für kurze Texte.

Codierung

- Ersetzen der Klartextes durch Bedeutungsgleiche Wörter/Symbole.
- Beispiel:
  - Schläfer: ein bestimmtes Wort auf öffentlichen Kanälen löst vorher besprochen Aktionen aus.
- Vorteile:
  - für kurze Bedeutungen sehr geeignet.

    - praktisch nicht zu knacken.
- Nachteile:
    - große Codebücher nötig
    - hoher logistischer Aufwand
- Fallbeispiel: Der Navajo-Code:
    - Einsatz von amerikanischen Ureinwohnern als Funker im zweiten Weltkrieg.
    - Die Navajos als einziger Stamm nicht von deutschen Forschern besucht.
    - Sprachfamilie Na-Dene: keine Verwandtschaft zu asiatischen oder europäischen Sprachen.
    - Klick-, Schnalz- und Klicklaute; komplixierte Konjugation der Verben
    - Lexikon für 274 militärische Begriffe
        - Jagdflugzeug - Kolibri
        - Aufklärer - Eule
        - Bomben - Eier
        - Schlachtschiff - Wal
        - Zerstörer - Hai
    - Übermittlung von Namen durch buchstabieren mit englischen Begriffen und einzelner Übersetzung
      Einsatz von Homophonen
    - später Ergänzung weiterer Begriffe im Lexikon
        - Deutschland - Eisenhut
        - Groß Brittanien - umgeben von Wasser
        - China - geflochtenes Haar
    - keine Codebücher; sehr schnell; fälschungssicher; nicht angreifbar
    - einer der wenigen Codes, der nie geknackt worden ist.

Chiffre - monoalphabetisch

- Julius Cäsar
    - Gallischer Krieg: Ersetzung der röm. Buchstaben durch griechische
    - Cäsar Chiffre
    - Exhausive Key Research
- 4 Jhd v Chr:
    - Kamasutra empfiehlt Frauen die Kunst der Kryptographie
    - Zufälllige Permutation des Alphabets als Schlüssel
    - Schlüsselwort
    - Bijektion zwischen Klartext- und Geheimtextalphabet
    - ca. 4e26 mögliche Schlüssel
- Al-Kindi 6 Jhd n Chr:
    - Versuch arabischer Theologen Überlieferungen islamischer Offenbarungen zeitlich einzuordnen.
    - Analyse der Worthäufigkeit => Zuordnung zu bekanntem Sprachgebrauch bestimmter Zeiten.
    - Häufigkeitsanalyse
        - je mehr Text, desto besser
        - liefert Ansätze für sprachliche Analyse
    - Entwicklung in Europa im 15.Jhd
- Gegenmaßnahmen:
    - Füller, Duplizierer, Löscher
    - Verfälschung des Textes: Buchstaben weglassen, Wörter falsch schreiben.
    - Codewörter => Nomenklator
    - Homophone Verschlüsselung: Gleichverteilung der Häufigkeit durch mehrere Symbole für einen Klartextbuchstaben
      => erschwert Analyse; ändert aber nichts am Prinzip, geknackt werden zu können.

Jedes Symbol steht für genau einen Buchstaben: Injektive Abbildung

Maria Stuart

- 1542/12/07: Geburt in Linlithgow bei Edinburgh
- 1543/11/09: Krönung am 9.11.1543 zur Königin der Schotten
- 1558: Hochzeit mit dem französischen Thronfolger Franz II. zur Festigung des Bündnisses gegen die englische Krone
- 1560: Krankheitsbedingter Tod von Franz II.
- 1565: Hochzeit mit Heinrich Stuart, dem Earl von Darnley: Sohn Jakob
- 1567: Mord an Darnley durch schottische Adlige
- Heirat mit James Hepbrun, dem vierten Earl von Bothwell
- Machtübernahme der protestantischen Adligen: Abdankung Marias zu Gunsten ihres Sohnes
- 1568: Flucht aus der Gefangenschaft. Letzter Versuch der Machtübernahme mit 6000 Royalisten. Niederlage bei Langside.
- Flucht nach England. Gefangennahme durch ihre Kousine Königin Elisabeth I.
- Für den katholischen Adel war Maria die rechtmäßige Thronfolgerin Englands.
- Nach 18 Jahren Gefangenschaft Kontaktaufnahme durch Anhänger auf dem Kontinent ins Chartley Hall in Staffordshire
- Das Babington-Komplott
    - Zentrale Figur: Anthony Babington.
      Großer Hass gegen das protestantische Establishment
    - Plan: Befreiung Marias, Ermordung Elisabeths, Sturz des Regimes unterstützt durch Invasion von außen.
    - Verwendung eines Nomenklators
    - Verstecken der Botschaften in einem hohlen Spund eines Bierfasses.
    - Überbringung durch Gilbert Gifford: ein Agent der englischen Krone.
    - Entschlüsselung durch Thomas Phelippes mittels Häufigkeitsanalyse.
    - Täuschung Babington's durch angeblichen Brief von Maria => Bekanntgabe aller Beteiligten
    - Hinrichtung der Verschwörer. Hinrichtung Maria's am 8.2.1587 in Fotheringhay Castle

Die Große Chiffre

- Antoine und Bonaventure Rossignol: Kryptoanalytiker unter Ludwig XII, VIV; 17Jhd
- Entwickler der Großen Chiffre; Dokumentation staatlicher Aktivitäten
- Etienne Bazeries, franz. Offizier
    - Dechiffrierung von 1890 - 1893
    - 587 verschieden Zahlen: keine Homophone; keine Bigramme
    - Silbensubstitution: 124-22-125-46-345 => les-en-ne-mi-s
    - manchmal Buchstabensubstitution, Füller, Löscher
    - Mythos: Mann mit der eisernen Maske; Zwillingsbruder von Ludwig XIV, Vorfahre Napoleons
      Befehlsverweigerer Vivien de Bulonde.

Polialphabetische Verschlüsselung

- le chiffre indechiffrable
    - Idee von Leon Battista Alberti, Florentiner Mathematiker, 15.Jhd: polialphabetische Verschlüsselung
    - weitere Abhandlungen durch Johannes Thrithenius, Giovanni Porta
    - Entwicklung zu einem System von Blaise de Vigenere

- Schwarze Kammer Wien, Seulen der Sehnsucht, Maria Stuart
- Charles Babbage
    - Tachometer, Kuhfänger, Jahresringe => Klima, Statistik: Sterblichkeitstabellen, Einheitspreise für Briefmarken
    - Differenzmaschine No1 und No2: erster Entwurf eines Computers
    - Wettstreit: Vigenere ist nicht neu
    - Zerlegen in Teilprobleme: Ermitteln der Periodizität; einzelne Häufigkeitsanalyse
    - Entdeckung nicht veröffentlicht
    - Wiederentdeckung durch Friedrich Wilhelm Kasaki, preusischer Offizier, 1863
- One Time Pads - der heilige Gral der Kryptographie
    - Unter bestimmten Voraussetzungen ist Vigenere nicht zu knacken:
        - Zufallsfolge als Schlüssel
        - Schlüssellänge = Textlänge
        - einmaliger Gebrauch
    - Jeder gewünschte Klartext kann beim Entschlüsseln gewonnen werden
    - Einsatzbeispiel XOR Verschlüsselung
    - Einführung 1918
    - hoher logistischer Aufwand: unpraktikabel
    - der heiße Draht: Washington - Moskau

Das Zimmermann-Telegramm

- Neutrale Haltung der USA unter Woodrow Wilson in den ersten beiden Jahren des 1. Weltkrieges.
- Befehl des Kaisers für uneingeschränkten U-Boot Krieg ab 1.2.1917 zur Aushungerung Englands. Jedoch Kriegeintritt der USA zu erwarten.
- Zimmermann's Plan:
    - Bündnis mit Mexiko: Zusicherung der Gebiete Texas, Neumexiko und Arizona. Finanzielle und militärische Unterstützung.
    - Japan veranlassen, die USA von Osten her anzugreifen.
    - Bedrohung von Westen durch deutsche Seemacht.
      => Beschäftigung der USA auf eigenem Gebiet => Sieg über Alliierte in Europa
- Nachricht über fremde Verbindungen nach Mexiko über Bootschaft in Amerika geschickt.
- Nachricht abgefangen und an Room 40 weitergeleitet.
- Entschlüsselung durch William Montgomery und Nigel de Grey.
- Verheimlichung der Entschlüsselung um Informationsquelle nicht trockenzulegen.
- Die USA bleiben überraschenderweise neutral; Das Zimmermann-Telegramm wird Wilson doch gezeigt.
- Gezielter Klau der mexikanischen Version und Veröffentlichung in der Weltpresse.
  Scheinbare Kritik in der britischen Presse über das Versagen des britischen Geheimdienstes.
  => Deutschland glaubt an Verrat in Mexiko, Room 40 bleibt im Hintergrund, USA tritt in den 1. Weltkrieg ein.

ADFGVX Verschlüsselung

- Einführung 5.März.1918
- Anfang Juni 1918 stehen die Deutschen kurz vor Paris
- Leutnant Georges Painvin knackt ADFGVX im speziellen
- Angriffspunkt bekannt => Alliierte verstärken Frontabschnitt => Deutsche werden zurückgeworfen
- allgemeine Lösung durch William Friedman:
    - 1) mind 2 Nachrichten mit gleichem Klartextanfang => Durchbrechung der Transposition
    - 2) mind 2 Nachrichten mit gleichem Klartextende => Durchbrechen der Abschirmung durch die Substitution
    - 3) Nachrichten mit genau gleicher Textlänge

Enigma

- Erfinder: Arthur Scherbius
- 3 Scheiben => 26^3 = 17576 mögliche Schlüssel
- 6 Walzenlagen => 105456 Möglichkeiten
- Vertauschung von 6 Buchstaben => 100.391.791.500
  => ca. 10e16 mögliche Schlüssel
- ab 1926: Einsatz im dt. Militär
- Polen ist in der Zange zwischen Russland und Deutschland
  =>Einrichtung des Biuro Szyfrow
- französicher Spion besorgt über deutschen Verräter, Hans-Thilo-Schmidt, Unterlagen zur Enigma und gibt sie an Polen
  - Nachbau eigener Enigma
  - Spruchschlüsselverfahren
- Marian Rejewski: bricht die Enigma-Chiffre über Fingerabddruck des Tagesschlüssels
- Bombe: mechanisierte Entschlüsselung

Bletchley Park

- 1939: neue Enigma: drei aus fünf Walzen (60 Lagen * 17576 Stellungen = 1.054.560 Schlüssel) , zehn Steckkabel => 1,59e20 Schlüssel
- Weitergabe des Know-Hows an Frankreich und Groß Britanien.
- 1.9.1939: Invasion der Deutschen in Polen
- Bletchley Park:
  - Mathematiker, Naturwissenschaftler, Linguisten, Philosophen, Schachgroßmeister, Kreuzworträtselsüchtige
  - Ausbau von 200 auf 7000 Mitarbeiter in 5 Jahren
  - Rejewski's Methode mit vielen Bomben
  - Ausnutzung von Cillies
  - Ausschluß gleicher Walzenlage => Halbierung des Schlüsselraums
  - keine Steckverbinder zwischen Nachbarn => Reduzierung der Schlüssel
  - Chosen Plaintext Attack: Aussetzen von Minen, Abfangen der Warnmeldungen deutscher U-Boote: "Gärtnern"

Alan Turing

- 1912/06/23: Geburt in Paddington, London
- 1926-31: Sherborne School
- 1931-34: Student am King's College, Cambridge Universität
- 1936: Die Turing Maschine
- 1939-40: Die Bombe
  - Änderung des deutschen Protokolls erwartet; neue Möglichkeiten gesucht.
  - Ausnutzung von Cribs, Known Plaintext Attack. Wetterbericht um 0600 Uhr.
    Schwäche von Enigma, dass Chiffre nie gleich Klartextbuchstabe ist (Reflektor)
  - 14.Mai.1940: Victory: erste Bombe, zu langsam
  - 10.Mai.1940: Keine Wiederholung des Spruchschlüssels mehr
  - 8.Aug.1940: Agnus Dei (Agnes): zweite Bombe
  - Bau von 15 Bomben in 1,5 Jahren
  - Ende 1942: Betrieb von 49 Bomben
  - Rekrutierungskampagnen

- 1952: Inhaftierung wegen Homosexualität
- 1954: Selbstmord durch Zyanid-Apfel in Wilmslow, Cheshire

Lorenz Chiffre

- Verschlüsselung der Kommunikation zwischen Hitler und seinen Generälen
- Prinzipiell ähnlich zur Enigma, jedoch komplexer
- individuelle Anpassungen beim Decodieren nötig
- Enturf von Colossus durch Max Newmann
- Bau durch Tommy Flowers
- erster Computer, Wiedergeburt der Differenzmaschine No 2
- nach dem WW vernichtet

symmetrische Kryptographie

- Luzifer-Chiffre, DES
- Verweis auf Vortrag von Stefan Schlott im Januar 2001

assymmetrische Kryptographie

- Problem der klassischen Krypto, Schlüssel zu verteilen
  bei n Kommunikationsteilnehmern n * (n - 1) / 2 Schlüssel nötig
- 1976 Diffie-Hellman-Merkle Verfahren zur Schlüsselverteilung von Martin Hellman entdeckt
  Ausnutzung von Einwegfunktionen, hier Modulorechnung
- Idee der assymmetrischen (public key) Kryptographie von Diffie; Suche nach math. Funktion
- April 1977: Rivest entdeckte das Rivest-Shamir-Adlemann-Verfahren (RSA)
  Einwegfunktion Primfaktorzerlegung
- Idee der asymmetrischen Krypto bereits 1969 von Ellis
- 1973: Entdeckung von RSA durch Cocks
- 1974: Diffie-Hellmann-Merkle-Verfahren entdeckt durch Williamson
- Mitarbeit im Government Communications Head Quaters (GB) verhinderte Publikation

Pretty Good Privacy

- Entwicklung von Phil Zimmermann
- Einbau von Key-Generatoren, digitale Signaturen
- public key zur Schlüsselübermittlung zur symmetrischen Verschlüsselung des eigentlichen Textes
- Patentverletzung gegenüber RSA Data Security
- Anklage wegen illegalem Export von Waffen (schwere Krypto)
- Diskussion über schwere Krypto für Jedermann (Terrorismus contra Datenschutz)