Kryptografie – Informatik des Vertrauens

Linksammlung

Inhaltsverzeichnis

Thomas Schaller – E-Mail: t.schaller@gymnasium.ettenheim.de. – September 2011

Allgemeine Links

Inf-Schule.de: Kryptografie. URL:*http://inf-schule.de/kommunikation/kryptologie*

Cryptool: Lehrerportal zu Cryptool. URL:*https://www.cryptoportal.org/*

Cryptool: Historie der Kryptographie - Überblick. URL: *https://www.cryptool.org/de/ctp-lehre/ctp-historie-de/261-ctp-history-zeittafel*

Cryptool: Schülerkrypto. URL: *https://www.cryptool.org/schuelerkrypto/*

ZUM-Wiki: Kryptographie. URL: *http://wikis.zum.de/zum/Kryptographie*

Uni Passau: Kryptographie und Schule. URL: *http://symbcomp.fim.uni-passau.de/symbolic-computation/schule-und-uni/schulkooperationen/kryptographie-und-schule/*

Laging, Hauke: Krypto für alle. URL: *http://www.crypto-fuer-alle.de/*

etoys-und-schule.de: Kryptografie. URL: *http://etoys-und-schule.de/krypto.pdf*

Hempel, Tino: Kryptografie. URL: *http://www.tinohempel.de/info/info/kryptografie/*

Gymnasium Am Thie: Kryptografie. URL:
http://www.gat-blankenburg.de/pages/fach/info/krypto.htm

Gymnasium Neustadt am Rübenberge: Kryptographie. URL:
http://gym-neu.dyndns.org/~hws/crypt/crypt.html

Universität Wuppertal: Spioncamp. URL: *http://ddi.uni-wuppertal.de/material/spioncamp.html*

OSZ Handel: Kryptologie.
URL: *http://www.oszhandel.de/gymnasium/faecher/informatik/krypto/index.htm*

Bundesnachrichtendienst: Ein kurzer Abriss zur Geschichte der Kryptologie.
URL: *http://www.bnd.bund.de/DE/Themen/Lagebeitraege/Kryptologie/Krypto_node.html*

Bundesnachrichtendienst: Beispieltexte - Lösungseinsendung an den BND. URL:
http://www.bnd.bund.de/DE/Themen/Lagebeitraege/Kryptologie/Unterpunkte/Kryptologiebeispiel_node.html

Universität Tübingen: Kryptologie. URL:
http://www-ti.informatik.uni-tuebingen.de/~reinhard/krypto/German/deutsch.html

Stobitzer, Christian: Kryptowissen.de URL: *http://www.kryptowissen.de/*

Brätz, Marcel: Kryptographiespielplatz.de URL:
https://www.kryptographiespielplatz.de/index.php

RWTH Aachen: Die Suche nach dem verlorenen Schatz. URL:
http://schuelerlabor.informatik.rwth-aachen.de/modul/die-suche-nach-dem-verlorenen-schatz-kryptographieverschluesselung-0

Wettbewerbe

PH Karlsruhe: Krypto im Advent. URL: *https://www.krypto-im-advent.de/*

Krypto-Wettbewerb. URL: *www.mysterytwisterc3.org*

Videos

itarchiv.net: Verschlüsselungsverfahren. (5min)
URL: *https://www.youtube.com/watch?v=HihZ6PKk9WI*

Krypto im Advent: Youtube-Kanal.
URL: *https://www.youtube.com/channel/UC6Gsk-HI73Wz8z_OP1SCDnw*

Spannagel, Christian: Verschlüsselung. Playlist.
URL: *https://www.youtube.com/playlist?list=PL6_AeYXBHF0OWS1GxV6lfivdReSyKhv3l*

Planet Wissen: Rätselhafte Botschaften. (58min)
URL: *https://www.youtube.com/watch?v=W4eguwkknyg*

Tools

Esslinger, Bernhard: Cryptool. URL: *https://www.cryptool.org/de/*

Strauch, Markus: Quick Sequence Diagram Editor. URL: *http://sdedit.sourceforge.net/*

Codeplex: VeraCrypt. URL: *https://veracrypt.codeplex.com/*

Symmetrische Verfahren

Inf-Schule.de: Symmetrische Verfahren - Einführung. URL:
http://inf-schule.de/kommunikation/kryptologie/modernechiffriersysteme/einstieg_symmetrischeschiffriersystem

Caesar

Inf-Schule.de: Chiffrierung mit dem Verschiebeverfahren. URL:
http://inf-schule.de/kommunikation/kryptologie/historischechiffriersysteme/station_verschiebeverfahren

Inf-Schule.de: Kryptoanalyse beim Verschiebeverfahren.
URL: *http://inf-schule.de/kommunikation/kryptologie/historischechiffriersysteme/station_kryptoanalyseverschiebeverfahren*

Matheprisma: Cäsar-Chiffren.
URL: *http://www.matheprisma.uni-wuppertal.de/Module/Caesar/index.htm*

Gymnasium am Thie: Die Caesar-Chiffrierung.
URL:*http://www.gat-blankenburg.de/pages/fach/info/caesar.htm*

Wikipedia: Caesar-Verschlüsselung.
URL: *https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsselung*

Universität Tübingen: Caesar-Chiffre.
URL: *http://www-ti.informatik.uni-tuebingen.de/~reinhard/krypto/German/3.2.d.html*

Videos

Spannagel, Christian: Caesar-Verschlüsselung. (15min)
URL: *https://youtu.be/mn-b36ax4PQ?list=PL6_AeYXBHF0OWS1GxV6lfivdReSyKhv3l*

Krypto im Advent: Caesar-Verschlüsselung. (4min)
URL: *https://www.youtube.com/watch?v=uFFt9XgQDK8*

Transposition

Gymnasium Am Thie: Die Transpositionschiffrierung.
URL: *http://www.gat-blankenburg.de/pages/fach/info/transpos.htm*

Wikipedia: Transposition. URL: *https://de.wikipedia.org/wiki/Transposition_(Kryptographie*)

Substitution

Müller, Oliver: Substitutionsverfahren.
URL: *http://www.cogito-ergo-sum.org/index.php/de/cryptography/83-krypto0*

Universität Tübingen: Substitutions-Chiffre.
URL: *http://www-ti.informatik.uni-tuebingen.de/~reinhard/krypto/German/3.3.d.html*

OSZ Handel: Substition - Tansposition.
URL: *http://oszhdl.be.schule.de/gymnasium/faecher/informatik/krypto/substitution.htm*

Vigenère

Inf-Schule.de: Chiffrierung mit dem Vigenère-Verfahren. URL: *http://inf-schule.de/kommunikation/kryptologie/historischechiffriersysteme/station_vigenereverfahren*

Gymnasium Am Thie: Die Vigenère-Verschlüsselung.
URL: *http://www.gat-blankenburg.de/pages/fach/info/vigen.htm*

Wikipedia: Vigenère-Verschlüsselung.
URL: *https://de.wikipedia.org/wiki/Polyalphabetische_Substitution#Vigen.C3.A8re-Verschl.C3.BCsselung*

Universität Tübingen: Vigenère-Chiffre.
URL: *http://www-ti.informatik.uni-tuebingen.de/~reinhard/krypto/German/3.5.d.html*

Cryptool Online: Autokorrelation. URL: *http://www.cryptool-online.org/index.php?option=com_content&view=article&id=90&Itemid=107&lang=de*

Wikipedia: Kasiski-Test. URL: *https://de.wikipedia.org/wiki/Kasiski-Test*

Videos

Krypto im Advent: Vigenère Verschlüsselung. (4min)
URL: *https://www.youtube.com/watch?v=4y4nCG8631g*

s41b0tproductions: Kryptologie - Vigenere Code mit Calc (6min)
URL: *https://www.youtube.com/watch?v=Bc7I9tD4PuA*

Michael Seidel: Vigenère und Kasiski. (6min)
URL: *https://www.youtube.com/watch?v=Y6qimy9o3f4*

Spannagel: Vigenère-Verschlüsselung. (11min)
URL: *https://www.youtube.com/watch?v=u6i4kKzeOWA*

Enigma

Matheprisma: Enigma.
URL: *http://www.matheprisma.uni-wuppertal.de/Module/Enigma/index.htm*

Videos

René Bohne: dorkbot Aachen #41: Roger Leifert - "Enigma Chiffriermaschine" (30min)
URL: *https://www.youtube.com/watch?v=6uZU4lpah5E*

Digital Brainstorming: Mythos Enigma - die Faszination der Chiffriermaschinen (9min)
URL: *https://www.youtube.com/watch?v=6130ch7KRsI*

Homophone Chiffren

Wikipedia: Homophone Verschlüsselung.
URL: *https://de.wikipedia.org/wiki/Homophone_Verschl%C3%BCsselung*

Cryptool: Homophone Chiffre. URL: *http://www.cryptool-online.org/index.php?option=com_content&view=article&id=68&Itemid=78&lang=de*

OTP

Inf-SChule.de: One-Time-Pad. URL:
http://inf-schule.de/kommunikation/kryptologie/historischechiffriersysteme/station_onetimepad

Gymnasium Am Thie: Das One-Time-Pad.
URL: *http://www.gat-blankenburg.de/pages/fach/info/one.htm*

Wikipedia: One-Time-Pad. URL: *https://de.wikipedia.org/wiki/One-Time-Pad*

Videos

Khan Academy: One-Time-Pad. (3min) URL: *https://www.youtube.com/watch?v=FIIG3TvQCBQ*

Jörn Loviscach: 07C.3 perfekte Verschlüsselung, One-Time Pad selbst programmiert (52min)
URL: *https://www.youtube.com/watch?v=Pt6I8laCx-I*

DES, AES

Matheprisma. DES. URL: *http://www.matheprisma.uni-wuppertal.de/Module/DES/index.htm*

Universität Tübingen: DES, AES.
URL: *http://www-ti.informatik.uni-tuebingen.de/~reinhard/krypto/German/deutsch.html*

Asymmetrische Verfahren

Inf-Schule.de: Asymmetrische Verfahren - Einführung. URL: *http://inf-schule.de/kommunikation/kryptologie/modernechiffriersysteme/einstieg_asymmetrischeschiffriersystem*

Gramm, Andreas: Vertraulichkeit durch asymmetrische Kryptologie herstellen URL: *http://it-lehren.de/asym/Vertraulichkeit-durch-asymmetrische-Kryptographie-herstellen.html*

CS Unplugged: Public Key Encryption. URL: *http://csunplugged.org/public-key-encryption/*

Applets zur modularen Arithmetik. URL: *http://www.saar.de/~awa/Applets_Mod_Arithmetik.html*

Videos

Gramm, Andreas: Vertraulichkeit durch asymmetrische Kryptologie herstellen (8min)
URL: *https://www.youtube.com/watch?v=nAXp7xbsAHE*

Modulare Arithmetik

Wikipedia: Kongruenz (Zahlentheorie).
URL: *https://de.wikipedia.org/wiki/Kongruenz_(Zahlentheorie)*

Rhein-Wied-Gymnasium Neuwied: Mathematische Grundlagen von RSA.
URL: *http://www.informatik.rwg-neuwied.net/sek2/krypt/rsa/page64/page64.html*

Embacher, Franz: Der erweiterte euklidische Algorithmus. URL: *http://www.mathe-online.at/materialien/Franz.Embacher/files/RSA/Euklid.html*

Videos

Muncan, Filip: Einführung in die Kryptographie Modulare Arithmetik (92 min)
URL: *https://www.youtube.com/watch?v=VU9Y0YN0XR8*

RSA

Matheprisma. RSA. URL: *http://www.matheprisma.uni-wuppertal.de/Module/RSA/index.htm*

Spiegel Online: Rekord-Entschlüsselung: Mathematiker knacken Zahl mit 200 Dezimalstellen.
URL: *http://www.spiegel.de/wissenschaft/mensch/rekord-entschluesselung-mathematiker-knacken-zahl-mit-200-dezimalstellen-a-355423.html*

Gymnasium Am Thie: Der RSA-Algorithmus.
URL: *http://www.gat-blankenburg.de/pages/fach/info/rsa.htm*

Mathe-online.at: RSA. URL: *http://www.mathe-online.at/materialien/Franz.Embacher/files/RSA/*

Inf-Schule.de: RSA. URL: *http://inf-schule.de/kommunikation/kryptologie/rsa*

Universität Tübingen: RSA.
URL: *http://www-ti.informatik.uni-tuebingen.de/~reinhard/krypto/German/deutsch.html*

mathematik.de: RSA -Verschlüsselung zum Ausprobieren. URL: *http://www.mathematik.de/ger/information/wasistmathematik/rsa/rsa_self.html*

Deininger, Matthias / RMG Haßfurt: Angriffe auf RSA (Facharbeit). URL: *http://wikis.zum.de/rmg/Benutzer:Deininger_Matthias/Facharbeit/Angriffe_auf_RSA*

Videos

Spannagel: RSA-Verschlüsselung. (60min)
URL: https://www.youtube.com/watch?v=IhDKJrXefXI

Spannagel, Christian: RSA: Ver- und Entschlüsselung (15min)
URL: *https://www.youtube.com/watch?v=LgAj4pGVIqI*

Spannagel, Christian: RSA: Konstruktion der Schlüssel. (17min)
URL: *https://www.youtube.com/watch?v=oXlY-yx1oIw*

Anwendungen

eMail

Inf-Schule.de: Sicherer E-Mail Austausch.
URL: *http://inf-schule.de/kommunikation/kryptologie/sichereremailaustausch*

Videos

SemperVideo: PGP Verschlüsselung - Theorie. (9min)
URL: *https://www.youtube.com/watch?v=RNZBzZuXZKk*

heinleinsupport: Im Stiftfilm erklärt: Wie funktioniert E-Mail-Verschlüsselung mit PGP? (3min)
URL: *https://www.youtube.com/watch?v=inxNRA4xK1Q*

Signaturen

Inf-Schule.de: Digitale Signatur.
URL: *http://inf-schule.de/kommunikation/kryptologie/digitalesignatur*

Gramm, Andreas: Integrität einer Nachricht und Authentizität ihres Absenders mit einer digitaler Unterschrift sicherstellen. URL: *http://ods3.schule.de/informatik/material/asym/Integritaet-und-Authentizitaet-mit-digitaler-Unterschrift-sicherstellen.html*

Zertifikate und Infrastruktur

Wikipedia: Man-in-the-Middle Angriff. URL: *https://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff*

Inf-Schule.de: Sicherheitsinfrastruktur.
URL: *http://inf-schule.de/kommunikation/kryptologie/sicherheitsinfrastruktur*

Wikipedia: Transport Layer Security.
URL: *https://de.wikipedia.org/wiki/Transport_Layer_Security*

Wikipedia: Web of Trust. URL: *https://de.wikipedia.org/wiki/Web_of_Trust*

Wikipedia: Public-Key-Infrastruktur. URL: *https://de.wikipedia.org/wiki/Public-Key-Infrastruktur*

Videos

SemperVideo: Web of Trust. URL: *https://www.youtube.com/watch?v=4HJ87iNkgX4*

SemperVideo: Man-in-the-Middle Angriff. (10min)URL: *https://www.youtube.com/watch?v=ZY1METeoEW8*

Weiterführendes

CCC: Zwischen supersicherer Verschlüsselung und Klartext liegt nur ein falsches Bit [30c3] (60min) URL: *https://www.youtube.com/watch?v=KxTh45_VhFk*

CCC: YouTube-Kanal. URL: *https://www.youtube.com/user/CCCdeVideos/videos*

Schneier, Bruce: Heartbleed.
URL: *https://www.schneier.com/blog/archives/2014/04/heartbleed.html*

Wikipedia: Heartbleed. URL: *https://de.wikipedia.org/wiki/Heartbleed*

Wikipedia: Secret-Sharing. URL: *https://de.wikipedia.org/wiki/Secret-Sharing*

Intypedia: Secret-Sharing Protocol. (15min)
URL: *https://www.youtube.com/watch?v=-wI5-uzSBdE*

CS Unplugged: Cryptographic Protocols. URL: *http://csunplugged.org/cryptographic-protocols/*

bitcoinblog.de: Kryptografie des Bitcoins. URL: *http://bitcoinblog.de/2013/12/22/kryptografie-des-bitcoins-fuer-anfaenger/*

Software

Sequenzdiagramm-Editor, mit dem die Sequenzidiagramme im Hintergrunddokument erstellt wurden: http://sdedit.sourceforge.net/download/index.html