Masarykova univerzita
Filozofická fakulta - Ústav hudební vědy
Teorie interaktivních médií
Jakub Mikuláš – 375 750

Cypherpunkeři

Stav diskuze a prostředků digitální kryptografie

2011

Obsah

Resumé

Práce sleduje vývoj prostředků na ochranu soukromí od kryptografie klasické po moderní. Vysvětluje vznik hnutí *cypherpunk*. Odpovídá na otázky „Proč se o cypherpunk/kryptografii zajímat?“, „Jaká témata cypherpunkeří řešili a jaká řešení nalezli?“ nebo „Potřebujeme cypherpunkery i dnes?“.

This paper pursues development of means to protect privacy from classical to modern cryptography. It explains the emergence of movement *cypherpunk*. Paper also tries to answers the question like "Why should we care about cypherpunk/cryptography?", "What topics cypherpunkers solve and what solutions they found?" or "Do we need cypherpunkers today?".

Úvod

Milan Kundera ve své knize *Nesmrtelnost* připomíná, že v křesťanském desateru neexistuje přikázání *„Nezalžeš!"*. Je to velmi zvláštní poznatek, že křesťan *nemá* povinnost říkat pravdu. Ale je vcelku logický, pokud Bůh stejně všechno ví – a ostatní lidé *nemají právo* se na nic ptát. Museli by se nejdříve zeptat, aby mohli požadovat pravdu. Kundera dále tuto myšlenku rozpracovává na moderní žurnalismus, ale mě spíše zaujala skutečnost, že lidská společnost nikdy nebyla *založena na nutnosti* říkat pravdu – vynechme prosím dystopické, utopické a totalitní systémy. A pokud společnost nemá nárok na pravdu, vzniká soukromí – tedy *možnost mít tajemství* a *možnost sdělit tajemství* (jen komu uznám za vhodné).

Ochrana soukromí je v nás však mnohem hlouběji než křesťanská nauka. Snad proto odedávna vznikaly technologie, které nás měly chránit pouze fyzicky, ale později sloužily i jako ochrana našeho soukromí a našich tajemství. Skrýše, dveře, zámky, sejfy a šifry – tyto a další technologie nás posunuly až k deklaraci práva na soukromí jako základního lidského práva[1].

Druhá půlka 20. století přichází s digitálními médii, která nás nutí přehodnotit dosavadní způsoby zajištění a ochrany soukromí. V této práci bych chtěl alespoň z části prozkoumat diskuze o soukromí a jejich aplikace ve věku výpočetní technologie.

1 Listina základních práv a svobod: Článek 7 : (1) Nedotknutelnost osoby a jejího soukromí je zaručena.

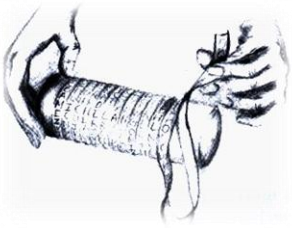
Stručné dějiny kryptografie a kryptoanalýzy

Jak jsem naznačil v úvodu, historie kryptografie zasahuje hluboko do minulosti, až někam do doby mezi 50 a 100 tisíci lety před naším letopočtem, kdy vzniklo abstraktní myšlení[2], které nám umožnilo uvažovat o *vlastnictví*. Něco co je jen vaše – jméno (které určuje váš vztah ke světu), myšlenka, předmět. Z vlastnictví vychází *soukromí*, tedy možnost jedince nebo skupiny selektivně odhalovat určitá vlastnictví – říct někomu své jméno, podělit se o nápad. Ve chvíli, kdy je tato úvaha možná, přichází čas pro další otázku – jak si své soukromí chránit? Jsou doloženy vaky a měchy pro ochranu osobního vlastnictví. Dalším důkazem jsou hroby a pohřebiště s osobními věcmi, které si zemřelí brali i do posmrtného života[3]. S domestifikací *(okolo roku 10 000 př.n.l)* vznikají ohrady, dveře a skrýše[4]. Později přicházejí zámky, sejfy a bezpečnostní systémy. A kryptografie je pouze rozšíření snah o ochranu soukromí.

Kryptografii jde v zásadě rozdělit na kryptografii klasickou a moderní. Ještě do roku 1949 jsme mohli mluvit o kryptografii klasické – tedy založené na čistě mechanickém principu. Moderní kryptografie pracuje s digitálními daty a bez použití výpočetních strojů je práce s ní téměř nereálná. Klasická kryptografie sahá několik tisíc let do minulosti – použití šifer v Mezopotánii a Egyptě není do dnes příliš jasné, ale od dob Řecka a Říma se můžeme skutečně bavit o kryptografii.

Klasická kryptografie

Historie šifer je od počátku silně provázaná s armádou. Šifry používali Sparťané[5], aby jimi předávali rozkazy a válečné zprávy. Jednalo se o jednoduchou transpoziční šifru, kdy se papír omotaný kolem válečku popsal a po jeho rozložení zůstala pouze řada náhodně vypadajících znaků. Dalším známým příkladem je klasická Caesarova šifra[6], která je snadno použitelná (i prolomitelná), ale občas se používá dodnes – jde o posun písmene v abecedě, takže z A je B, z B je C atd. Další zájem o kryptografii přichází v 19. století. Není náhoda, že ze stejné doby pochází i Baggageho *Difference Engine*. Kryptografii se dostává jak systematického zájmu ze strany matematiků tak i pozornosti širší veřejnosti - o kryptografii píše například i Edgar Allan Poe ve své povídce Zlatý brouk[7] z roku 1843 (Kryptografie zde hraje klíčovou roli pro rozluštění případu).



Větší zvrat nastává s příchodem druhé světové války. V této době již existovaly mnohé elektromechanické šifrovací systémy, avšak pozornost se věnovala především rozluštění Enigmy, která se používala již od 20. let 20. století. Právě její prolomení a praktické dopady práce kryptoanalytiků v Polsku a britském Bletchley Parku ukázaly na důležitost dobrého šifrování v armádě – nebo alespoň dobré kryptoanalýzy. Během války se toto potvrdilo ještě například v bitvě o Midway, kde prolomení japonské šifry[8] znamenalo rozdíl mezi výhrou nebo porážkou.

Moderní kryptografie

Od druhé světové války byly na tvorbu šifer *(především v USA*) vydávány obrovské sumy vládních peněz[9]. Do kryptografie investuje především námořnictvo a tajná služba. V roce 1949 vzniká útvar AFSA *(Armed Forces*

2 Modern human behaviour. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-26]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Modern_human_behaviour>.

3 ELIADE, Marcea. Dějiny náboženského myšlení : Od doby kamenné po eleusinská mystéria. 3. opr. vyd. Praha : OIKOYMENH, 2008. 518 s.

4 ELIADE, Dějiny náboženského myšlení

5 YOUNG, Gary De. Dr. Gary De Young [online]. X [cit. 2011-06-19]. Spartan Scytale. Dostupné z WWW: <http://courses.gdeyoung.com/pages.php?cdx=168>.

6 Caesar cipher. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-19]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Caesar_cipher>.

7 POE, Edgar Allan. Zlatý brouk. Praha : Argo, 2010. 108 s.

8 Cipher Machines [online]. 2006 [cit. 2011-06-14]. Japanese Purple Cipher. Dostupné z WWW: <http://ciphermachines.com/ciphermachines/purple.html>.

9 History of cryptography. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-20]. Dostupné z WWW: <http://en.wikipedia.org/wiki/History_of_cryptography>.

Security Agency), předchůdce dnešní National Security Agency *(NSA),* založené v roce 1952. V roce 1949 se však stala ještě jedna důležitá věc – vyšla kniha *Communication Theory of Secrecy Systems*[10]. Claude Shannon[11] – „*otec informačních technologií*" pracoval během Druhé světové války na projektech spojených s kryptografií a binární logikou. Jeho návrh řešení problémů booleanovy logiky v binárních systémech se stal základem pro práci pozdějších matematiků. Jeho práce je považována za počátek moderní kryptografie. Shannon navrhuje využití informačních technologií[12] pro lepší šifrování. Jeho výsledky velmi zaujaly AFSA – a tak se počítalo s tím, že (digitální) šifrování bude primárně armádní záležitostí. A skutečně tomu tak bylo – nejpokročilejší šifrování měla americká NSA a britská GCHQ (Government Communications Headquarters).

Polovina 70. let však přinesla změnu, kterou pociťujeme až dodnes. Nejdříve v roce 1976 vznikl Data Encryption Standard[13] – veřejná šifra vyvinutá IBM a propagovaná vládou a Národním institutem standardů a technologie. Bohužel se nikdy ve velkém neuchytila[14], částečně také ze strachu z backdooru[15], který by do ní teoreticky mohla umístit NSA, aby měla přístup k zašifrovaným datům. Důležité bylo, že sama vláda prosazovala standardizovanou šifru pro privátní sektor. Sama vláda chtěla, aby si občané *alespoň nějak* svá data *(jako firemní tajemství atd.)* šifrovali.

Druhým, mnohem důležitějším, zvratem byl vynález asymetrické *(public key)* kryptografie. Whitfield Diffie a Martin Hellman[16] přišli se systémem veřejného a soukromého (asymetrického) klíče, který zaručoval bezpečnou komunikaci i když byl komunikační kanál celou dobu konverzace odposloucháván. Co bylo však důležitější, tento systém nevyvinula žádná vladní organizace[17], ale lidé z civilního/akademického sektoru. S příchodem RSA[18] *(aplikace asymetrické kryptografie)* v roce 1978 měla veřejnost v ruce velmi silný nástroj pro ochranu soukromí. Dokonce tak silný, že jej nedokázaly prolomit ani vládní organizace. Což se samozřejmě vládě nelíbilo, uvalila tedy embargo na vývoz šifrovacích algoritmů delších než 40bitů *(což už v roce 1978 byla slabá šifra)*. Zákaz trval v podstatě až do roku 2000.

V tomto okamžiku je důležité si uvědomit, že v jednu dobu existovaly dva velmi protichůdné názory na použití kryptografie v civilním sektoru: na jedné straně vláda, která by ráda zamezila tomu, aby si kdokoliv mohl cokoliv zašifrovat tak, aby k tomu žádná vládní organizace neměla *teoretický* přístup. Na druhé straně je nově vznikající skupina, která by ráda měla kontrolu nad svým digitálním soukromím. Z druhé skupiny vznikne jakýsi odboj-hnutí:

Cypherpunk

10 SHANNON, Claude. Communication Theory of Secrecy Systems. New Jersey : Bell Labs, 1949. 60 s.

11 Claude Shannon. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-20]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Claude_Shannon>.

12 Je v tomto ohledu důležité si uvědomit v jaké fázi vývoje byly informační systémy v roce 1949

13 SMID, Miles; BRANSTAD, Dennis. The Data Encryption Standard : Past and Future. Proceedings of the IEEE. 1988, s. 43-65.

14 Používala se pouze asi do poloviny 80. let

15 Nedokumentovaná cesta, jak napadnout systém. V případě DES byl problém v *podezřelých* code blocích

16 Oba byli součastí hackerské komunity na MIT v 60. letech

17 I když Bobby Inman (bývalý ředitel NSA) oznámill, že NSA měla Public Key již v roce 1966 (viz. The Cyphernomicon níže)

18 Algoritmy.net [online]. 2011 [cit. 2011-06-29]. Algoritmus RSA. Dostupné z WWW: <http://www.algoritmy.net/article/4033/RSA>.

Cypherpunkeři

Cypherpunkeři byli většinou technicky znalí uživatelé, kteří měli aktivní vztah k matematice a výpočetním technologiím. Možnost aktivně participovat v boji proti *policejnímu státu*, jak jej ukazuje Orwell, pro ně byla revoluční myšlenkou. Studená válka nevypadala, že by měla skončit a s trochou fantazie se mohla přirovnat k *Udržovací válce*. Právě tito lidé a právě v takové době *zničehonic* disponovali nástroji, které jim dovolovaly obranu proti všemožným vládním aktivitám zaměřeným proti jejich soukromí.

> I zákony proti kryptografii sahají pouze tak daleko, kam státní hranice a násilí.
> Eric Hughes - Cypherpunk's manifesto[19]

Historii, důležité postavy a souboje cypherpunkerů a vlády popisuje Steven Levy v knize *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*[20]. Bylo to období skutečné války mezi cypherpunkery a NSA. NSA chránila monopol na kvalitní kryptografii a národní zájmy – cypherpunkeři bojovali spíše za ideály, než za nějaké konkrétní *(revoluční)* myšlenky. Mnoho prominentních cypherpunkerů skončilo ve vězení[21]. Cypherpunkeři nikdy nebyli nijak organizovaní a jejich názorové spektrum zasahovalo od krajní levice přes krajní pravici až po anarchismus[22]. Cypherpunkery ze začátku spojoval především zájem o *civilní kryptografii,* public key a možnosti nasazení kryptografie v reálném životě. Další témata přišla až na konci 80. let a začátku 90. Základní sdílená ideologie cypherpunkerů byla postavena na knihách jako Orwellův 1984, The Shockwave Rider, True Names[23], Ender's Game, Snowcrash, The Cryptonomicon nebo The Puzzle Palace. A samozřejmě odborná literatura o kryptografii a matematice a velké množství čistě cyberpunkových textů.

Avšak na důležitosti cypherpunkeři skutečně získali až v roce 1992. Vznikl totiž *Cypherpunk mailing list*. Mailing list[24], který svými tématy o několik let předběhl dobu. Vznikl v San Franciscu z iniciativy Erica Hughese[25], Timothy C. Maye[26] a Johna Gillmora[27]. Všichni 3 byli finačně zajištění a úspěšni ve svých oborech. Založili si malý *diskuzní kroužek*, který se scházel jednou měsíčně v kanceláři Johna Gilmora. Z těchto mítinků pochází i označení *Cypherpunk*[28], který vymyslel Jude Milhon[29]. Brzy po prvním setkání vznikl Mailing list. Diskuze cypherpunkerů se stále točily kolem posledního vývoje v oblasti techniky, tím se nelišily od jiných technicky zaměřených mailing listů, rozdíl byl v přítomnosti diskuze o ochraně soukromí v digitální době, o nebezpečí policejního státu a o změnách, které mohou přijít. Přispěvatelé mailing listu[30] byli především odborníci, od čehož se odvíjela i úroveň diskuze.

19 HUGHES, Eric. Activism.net [online]. 1993 [cit. 2011-05-29]. A Cypherpunk's Manifesto. Dostupné z WWW: <http://www.activism.net/cypherpunk/manifesto.html>.

20 LEVY, Steven. Crypto : How the Code Rebels Beat the Government Saving Privacy in the Digital Age. [s.l.] : Penguin, 2002. 368 s. ISBN 978-0140244328.

21 Například Jim Bell *(autor Assasination politics)* je v něm dodnes

22 Viz. Crypto-anarchismus jako ideologie postavená na kryptografii.

23 Ačkoliv jsou na kvalitu Vingeho povídky různé názory, na cypherpunkery zapůsobila velmi podmanivě. Což lze doložit na častém odkazování k textu v cypherpunkových textech. To, že si musíme chránit naše Pravé jméno je to, co cypherpunkery velmi vystihuje.

24 Mimochodem: dodnes funkční. Je to jeden z nejdéle funkčních mailing listů - cypherpunks@al-qaeda.net mailing list původně vznikl pod doménou toad.com – ano, web Johna Gilmora

25 Matematik z Berkeley a autor A cypherpunk's manifesto

26 Matematik, výzkumník Intelu, autor The Cyphermoniconu, The crypto anarchist's manifesto a True Nyms and Crypto Anarchy. Výčet jeho důležitých textů by však byl mnohem delší.

27 Zakladatel Electronic Frontier Foundation, výzkumník u Sun Microsystems a známý aktivista.

28 Název je odvozen od populárního žánru: cyberpunk.

29 V hackerské komunitě známý také jako *St. Jude*. Editor časopisu Mondo 2000 (který zakládal)

30 http://www.cypherspace.org/adam/cp-stats.txt - seznam přispěvatelů mailing listu (nepodařilo se mi přímo zjistit data záznamu). Seznam obsahuje mnoho zajímavých jmen – Bruce Schneier, David Wagner, Adam Shostack, Steven Bellovin a

Jak poznamenal Will Rodger:

„Byla to směs revoluční politiky a pokročilé matematiky"
– Will Rodger[31]

Mezi *archaickými* cypherpunkery existovaly v podstatě 2 možnosti, jak bude vypadat budoucnost[32]:

1. Stát pomocí digitálních technologií a neustálého sledování zničí osobní svobodu a soukromí.
2. Nebo stát bude zničen (nebo alespoň minimalizován) za pomoci digitálních technologií jako kryptografie.

Ale témata se dotýkala i využití a zneužití technologií nebo úloha techniky pro běžného člověka. Nekompletní archiv mailing listu je stále k dohledání[33]. Dodnes obsahuje zajímavé podněty. Zajímavý je i pohled na počet odběratelů, který už v roce 1994 dosáhl 700 lidí a v roce 1997 (vrchol) až 2000 čtenářů. Pokud uvážíme, jaká byla penetrace inernetovým připojením mezi obyvatelstvem (až od roku 1997 se jednalo o 11% populace 1. světa)[34] a odbornost diskuze, jsou to čísla ukazující na opravdový zájem o tuto tématiku.

Kolem cypherpunku vzniklo několik velmi důležitých textů: předně *The Cyphernomicon*[35] – cypherpunkerský FAQ z roku 1994 o cypherpunku, cryptoanarchii a soukromí. Je to velmi obsáhlý a místy nepřehledný[36] dokument, který dává i po více než 15 letech možnost lépe se vcítit do jejich uvažování, kdy nikdo s nikým v podstatě nesouhlasí[37], ale všichni vědí, že přece jen sdílí určité ideály. Vcelku trefně poukazuje na cypherpunkery jako skupinu *počítačových punkerů*. The Cyphernomicon dále vysvětluje motivace pro vznik mailing listu atd. Obsahuje také rady ohledně kryptografie a etikety mailing listu.

A Cypherpunk's Manifesto také přináší několik zajímavých názorů:

Soukromí v otevřené společenosti vyžaduje kryptografii. Pokud něco řeknu, chci, aby to slyšeli jen ti, jimž je to určeno.
Eric Hughes – Cypherpunk's manifesto

Cypherpunkeři skutečně dlouhou dobu věřili v rychlé vítězství *individuálního* nad *státním*. Podporovalo je v tom zjištění, že public-key je největší vynález v oblasti kryptografie od renesance. A vznik PGP na počátku 90. let, který měl přiblížit kryptografii masám, je dále podporoval v jejich snažení. Stejně tak se často ve svých textech oháněli až *romantickými* představami o korporacích, policejních státech apod. Z cypherpunku lze často cítit aktivistická rétorika 90. let. Naštěstí se nedrží jen té, ale posunují diskuzi konstruktivnějším směrem.

samozřejmě i Julian Assange. Na listu lze najít i několik českých (ne však příliš důležitých) jmen.

31 RODGER, Will. SecurityFocus [online]. 2001 [cit. 2011-06-21]. R.I.P. Cypherpunks. Dostupné z WWW: <http://www.securityfocus.com/news/294>.

32 MANNE, Robert. Cryptome [online]. 2011 [cit. 2011-06-14]. The Cypherpunk Revolutionary Julian Assange. Dostupné z WWW: <http://cryptome.org/0003/assange-manne.htm>.

33 Mailing list ARChives [online]. 2001 [cit. 2011-06-21]. Dostupné z WWW: <http://marc.info/?l=cypherpunks>.

34 Internet users per 100 inhabitants 1997-2007 ITU.png. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-29]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Soubor:Internet_users_per_100_inhabitants_1997-2007_ITU.png>.

35 MIT Project on Mathematics and Computation [online]. 1994 [cit. 2011-06-10]. The Cyphernomicon. Dostupné z WWW: <http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ>.

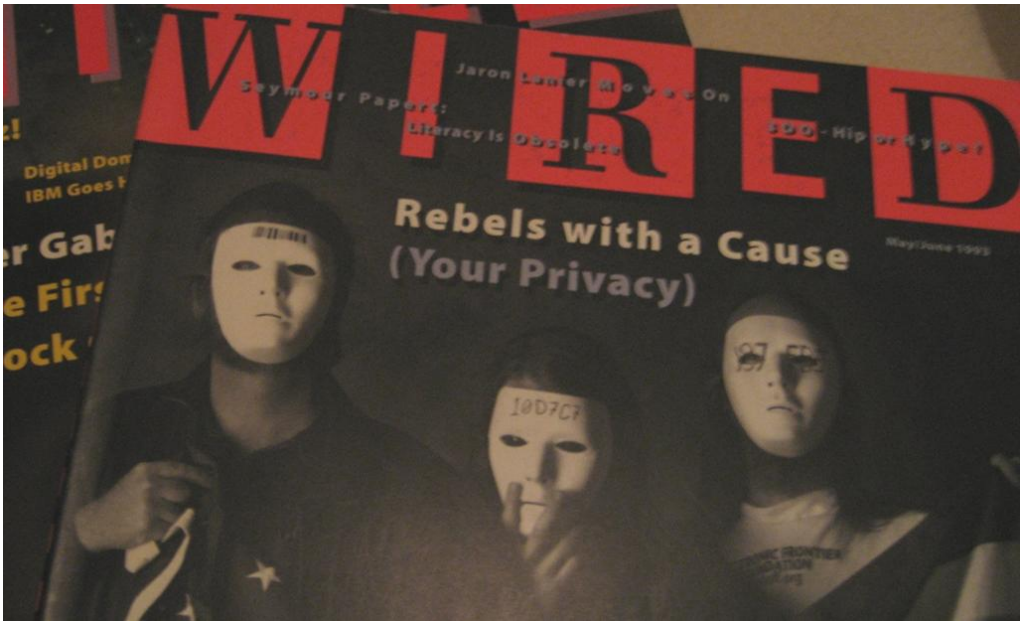
36 Přece jen, je to cypher*punkový* text

37 Mailing obsahoval z nemalé části i osobní útoky, hádky apod. – nutno říct, že si ale stejně udržovaly určitou úroveň

Cypherpunkeři píší kód. Víme, že někdo musí psát software na ochranu soukromí. A nebudeme mít soukromí, dokud to nebudeme dělat všichni, a proto ho budeme psát.
Eric Hughes - Cypherpunk's manifesto

„Cypherpunks write code" se stalo jakýmsi heslem cypherpunkerů. Další důležitý text vycházející z cypherpunkerské ideologie je *Assassination politics*[38]. Assassination politics Jima Bella je zajímavý myšlenkový experiment, který počítá se vznikem anonymního[39] *Dead Poolu*[40], který nám v konečném důsledku má přinést otevřenou společnost, minimální stát apod. Zajímavostí je, že vznikl také *pornofilm*, který vyšel v malém nákladu a pro cypherpunkery – *Cryptic seduction*[41]. Podle popisu je rozdíl mezi *klasickým* porno filmem a *krypto* porno filmem například v několika odkazech k *backdoorům*[42].

Důležitým bodem byl také článek *Crypto Rebels*[43] v tehdy začínajícím časopisu Wired – který cypherpunkerům přinesl větší podporu veřejnosti. Je to obsáhlý článek osvětlující důvody a způsob jejich vzniku. Obsahuje také vyjádření NSA k cypherpunkerům, informace o zatčení Johna Gillmora nebo zamyšlení nad budoucností cypherpunkerů v době přicházejících mobilních telefonů.



38 BELL, Jim. Outpost of Freedom [online]. 1997 [cit. 2011-06-14]. Assassination Politics. Dostupné z WWW: <http://www.outpost-of-freedom.com/jimbellap.htm>.

39 S použitím anonymních platebních metod, aby nebylo možno vystopovat účastníky

40 Seznam lidí, u kterých „tipujete" kdy zemřou. Správné uhádnutí se rovná výhře.

41 Mail-archive.com [online]. 2000 [cit. 2011-05-30]. CRYPTIC SEDUCTION -- CYPHERPUNK SPECIAL. Dostupné z WWW: <http://www.mail-archive.com/cypherpunks@algebra.com/msg04068.html>.

42 ORLOWSKI, Andrew. The Register [online]. 2002 [cit. 2011-05-30]. Alice, Bob and Eve too. Dostupné z WWW: <http://www.theregister.co.uk/2002/03/16/alice_bob_and_eve/>.

43 LEVY, Steven. Crypto Rebels. Wired 1.02. 1993, 1, 2. Dostupný také z WWW: <http://www.wired.com/wired/archive/1.02/crypto.rebels_pr.html>.

Současný cypherpunk

Cypherpunk nezanikl. Mailing list je stále aktivní a vzhledem k tomu, jaká je základna jeho přispěvatelů a fakt, že je moderovaný, udržuje si určitou úroveň. Od konce 90. let se termín přestal používat, ale jejich myšlenky přetrvaly. Objevovaly se nové projekty, koncepty a postupy při využívání kryptografie[44]. Co se primárně změnilo?

1. Rozšířenost internetu (trochu paradoxně) vedla k tomu, že nemůže vzniknout centralizovaná diskuze o kryptografii:
    a. buď bude skupina příliš malá, než aby měla nějaký hmatatelný efekt na globální diskuzi nebo snad i smýšlení.
    b. nebo je tak velká, že se diskuze rozpadá a ztrácí koncentraci na jedno (i když rozsáhlé) téma.
2. Téma šifrování *mimo-internet* se přesunulo do pozadí[45]. Může za to především kvalita dnes dostupných nástrojů pro šifrování[46]. Například svobodný software TrueCrypt je při správném použití v dnešní době neprolomitelný (neexistuje ani teoretická možnost prolomitelnosti šifry AES – navíc TrueCrypt umožňuje kombinovat více vrstev obrany)
3. Diskuze se také přenesla od *policejního státu*, který občany fyzicky kontroluje v jejich domech apod. k *policejnímu/korporátnímu kyberprostoru* – každý pokus o monitorování internetu přináší protesty a petice[47].
4. Poslední změnou je zjednodušení a zlevnění kryptografie. Jestliže v 90. letech byla kryptografie doménou armády, tajných služeb, matematiků a počítačových odborníků – dnes je šifrování přístupné i pro méně zasvěcené. A právě toto byl jeden z cílů cypherpunků – vytrhnout kryptografii vládě a dát ji uživatelům, aby se mohli bránit před kontrolou, opresemi nebo nátlakem. Kryptografie může být dnes velmi levná - pokročilý software jako TrueCrypt[48] je zdarma. Další šifrovací software je zdarma dostupný například pro OS Linux, který je také zdarma. I cena potřebného hardwaru klesla. Pro rychlou a bezpečnou práci se zašifrovanými soubory stačí i podprůměrný hardware. To samé platí i pro software, který nás má chránit na internetu – např. Vidalia[49] *(Tor + Privoxy + Firefox)* nebo I2P[50].

Cypherpunkeři v kyberprostoru

Prvně je nutné si uvědomit, *před kým* se vlastně máme v kyberprostoru bránit šifrováním. (1) Vlády, které cenzurují přístup k internetu[51]. Každou chvíli se objeví návrh na sledování uživatelů, omezení přístupu k *nebezpečným* webům. Ať už se tak děje kvůli válce proti terorismu, pedofilům nebo jen kvůli zdanění internetových kasin *(to se netýká jen ČR, podobné návrhy zaznívají i v USA, UK, Německu* atd.) (2) Bezpečnostní složky, které chtějí vědět, co děláte.

44 Zajímavý je například Assangeho systém Marutukku - Rubberhose (file system). In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-15]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Rubberhose_(file_system)>.

45 Nemyslím šifrování v *meatspace*, ale šifrování pevných disků apod. zařízení, která nejsou online

46 Za mnohými z nich stáli právě cypherpunkeři

47 Jak se mimochodem nedávno stalo i v ČR

48 TrueCrypt [online]. 2011 [cit. 2011-06-10]. TrueCrypt. Dostupné z WWW: <http://www.truecrypt.org/>.

49 Tor Project [online]. 2011 [cit. 2011-06-09]. Vidalia. Dostupné z WWW: <https://www.torproject.org/projects/vidalia.html.en>.

50 I2P [online]. 2011 [cit. 2011-06-10]. I2P Anonymous Network. Dostupné z WWW: <http://www.i2p2.de/>.

51 Internet censorship by country. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-21]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Internet_censorship_by_country>.

> Pokud vážně chceš posílat všechny své zprávy nezašifrované a skrz veřejné kanály, dobře. Ale nestěžuj si prosím, až zjistíš, že já (nebo kdokoliv jiný) si je čteme.
> – MrKite[52]

Mezi cypherpunkery platí, že pokud je komunikace nazašifrovaná, někdo cizí ji čte. Je to čistý racionální předpoklad, který počítá s tím, že číst nezašifrovanou komunikaci je velmi jednoduché (což skutečně je). A právě vlády mají zdroje monitorovat i velké objemy komunikace. Nebo si rovnou mohou zajistit přístup k vašim online službám[53]. Samozřejmě to platí analogicky i pro nebezpečí v podobě *black hat* hackerů, malwarů apod.

Jak se tedy dnes aplikují cypherpunkerské postupy? Co hmatatelného nám poskytl cypherpunk? Předně vznikly projekty jako TrueCrypt nebo Tor.

Tor

Tor[54] je anonymní síť založená na technologii Onion Routingu[55]. Její důležitost spočívá především

- v (relativně) nízké odezvě, díky čemuž se dá použít i k anonymnímu používání aplikací
- ve schopnosti spolupracovat v podstatě se všemi aplikacemi na všech důležitých operačních systémech
- v jednoduchém a rychlém nastavení. Doslova během několika minut můžete obejít vládní cenzuru nebo pomoct jiným uživatelům obejít cenzuru
- v ceně – je zdarma.

Tor dovoluje komunikaci jak pouze v rámci Tor sítě (chová se v tomto ohledu jako darknet[56]), ale i anonymní komunikaci na klasickém internetu.

Uvnitř Tor sítě

V Tor síti se nacházejí tzv. *Hidden services*, což jsou technicky vzato klasické webové servery, pouze s přidanou vrstvou anonymity. Komunikace sama v rámci Tor sítě je anonymnější a teoreticky nelze sledovat[57].

Nabídka takových služeb je vcelku široká. Knihovny, nabízející knihy od klasických až po návody na sestrojení výbušnin. Diskuzní fóra a stránky aktivistů, kteří mají strach z perzekuce. Občas lze najít i diskuzní fóra disidentských skupin. Odbornější technické diskuze nejsou přístupné bez *pozvánky* – obvykle pozvánka znamená URL[58] adresa. Vnitřní Tor síť je totiž v podstatě *čistý* hypertext, kdy se bez odkazu k dalšímu zdroji nikam nedostanete[59]. Při prvním příchodu na Tor vidíte jen stránky, které se implicitně zviditelňují[60]. Takže získávání informací dostává, paradoxně k tomu, že je to anonymní síť, více *lidský* rozměr, kdy se často musíte zeptat *někoho* a ne *mechanického* vyhledávače. Vnitřní Tor síť je tedy výborným místem pro různé niché-skupiny, které si nepřejí být rušeny a pro které je anonymita jen další plus. O jaké skupiny se jedná? Často to jsou pedofilové a jejich uzavřené komunity. Dále určité množství webů v neevropských jazycích – což zahrnuje informační body několika teroristických organizací[61], politické aktivisty a fóra s neznámým

52 Tachyon [online]. 2006 [cit. 2011-06-26]. [cspace-users] Re: Cspace. Dostupné z WWW: <http://lists.tachyon.in/pipermail/cspace-users/2006-August/001128.html>.

53 ICAZA, Miguel de. Miguel de Icaza [online]. 2011 [cit. 2011-06-23]. Dropbox Lack of Security. Dostupné z WWW: <http://tirania.org/blog/archive/2011/Apr-19.html>.

54 Tor Project [online]. 2011 [cit. 2011-06-09]. Dostupné z WWW: <https://www.torproject.org/ >.

55 Onion routing. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-28]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Onion_routing>.

56 Zvenčí nepřístupná síť

57 Existují pouze modely sledování založené na statistických modelech sledování provozu a jeho rozložení. Stále se zkoumají.

58 Vzhledem k tvaru odkazů v Tor síti (např. The Hidden Wiki - http://kpvz7ki2v5agwt35.onion) je nepravděpodobné, že by někdo zvenčí náhodně objevil funkční web.

59 Existovaly pokusy zavést vyhledávací engine v Onionlandu (označení pro darknetovou složku Tor sítě), ale ty vždy zkrachovaly a k dnešnímu dni nefunguje ani jeden.

60 Na rozdíl od internetu, kde nejdou vidět ty weby, které se skrývají. Stránky, které se propagují, jsou často s pornografickým obsahem, proto mnoho lidí po příchodu do Onionlandu nabývá dojem, že Tor je jen síť pro sdílení (pedofilní) pornografie

61 Na Tor fóru talk.masked se nějakou dobu diskutovalo o pravosti těchto webů – samozřejmě se ukázalo, že je nemožné to potvrdit nebo vyvrátit

obsahem. V Onionlandu mají zastoupení také 2 české projekty: PirateLeaks.cz[62] a KinderPorno.cz[63].

Podle několika zdrojů, které provedly analýzu provozu na Toru, je však většina provozu směřována ven ze sítě do *normálního* internetu. Jde tedy vidět, že většině uživatelů stačí *normální* internet, jen ho chtějí používat anonymně. Lepší odhady by však vyžadovaly výzkum Tor a I2P sítě v takovém rozsahu, v jakém doposud nebyly provedeny.

62 http://qyy2n2lqpc5l524q.onion:8080/

63 http://n4k727nqnwkvb4g6.onion/d/

"Everything you need to start the revolution"

Index

UPDATE: Looking for writers to make new articles and recipes, email havocnet1337@gmail.com

Explosives

- Thermite
- Thermate
- Molotov cocktail
- Smoke Grenade
- Cluster Bomb

Hacking IRL

- Electronic road signs
- Hot-wire a car

Internet Hacking

Drugs

How to

- Choose a handgun
- Dispose a body

Explosives

Thermite

Materials:

Iron Oxide
Aluminium Powder

TorDir

The link list /AND PM SYSTEM/ of Tor

Search

Username: Password: Login

Home | Add a Link | Register

Now this site also provide a Private Messaging System with good privacy features including a "friends-only" whitelist method. You may register to get your inbox.

You may also contact us, if need, by PM to **tordir** with our PM system (you need to be registered to can send or receive PM's)

We're sorry for some issues latelly on access this site, it was due to a clock malfunction causing SSL and Tor to fail. We'd been fixing it and believe it's alright now.

- Activism, Political and Revolutionary — 6 links in this category
- Adult — 26 links in this category
- Business — 11 links in this category
- Email, IM, Communications — 8 links in this category
- Gambling — 3 links in this category
- Hacking and Related — 4 links in this category
- Librarys — 6 links in this category
- Reference and Core sites — 2 links in this category
- Security
- Social
- Social File/happiness sharin

8c5f1d9e71a
986616ba3f7
3bbfca03408

РусьИнфо

РУССКОЕ ИНФОРМАЦИОННОЕ АГЕНТСТВО

Русские новости	Русская идеология
Юрий Буданов: последний урок	Северное Братство и финансирование наших проектов. Часть 3

Сегодня около полудня на Комсомольском проспекте в Москве при выходе из нотариальной конторы застрелен бывший полковник Юрий Буданов. Ответ на вопрос, кто это сделал, на мой взгляд, лежит на поверхности - либо сами родственники Эльзы Кунгаевой наняли киллеров, либо то же самое сделали другие чеченцы. Стоит отметить, что в адрес Буданова регулярно звучали угрозы как в виде заявлений официальных лиц Чечни, так и в виде звонков с угрозами расправы. Уже после убийства чеченский депутат Адам Делимханов назвал случившееся "возмездием". Конечно, можно предположить, что убийство экс-полковника - это какая-то хитрая политическая игра спецслужб, однако в данном случае мотивов устранять подобную провокацию лично я не наблюдаю. Наоборот, все гораздо проще и истина лежит на поверхности. Хотя в том, что официальные лица Чечни

[..]

Комментарии: 4 — Сталкер — 2011-06-10 — Новости

Ресурсов Координационного Штаба хватает только на заложение Основ Сопротивления по всем описанным в первых двух частях направлениям. Это немало. Но недостаточно для развития Успеха. Команда разработчиков проекта не может его одновременно разрабатывать-профинансировать-реализовать самостоятельно, то есть без вас.

Без обретения новых сторонников и соратников, без обретения финансирования дальнейшее успешное развитие Сопротивления невозможно. Но если мы до вас не достучимся, то ваши дети умрут от рук исламских фанатиков. Именно ваши. А не кого-то еще. Потому что вы, прочитав наши материалы, ЗНАЛИ ЧТО ДЕЛАТЬ, но так и не подняли ж.пу с дивана, проявив неоправданное сомнение, бездействие, трусость и малодушие. Тем не менее, опыт предшествующих революций показывает нам, что набор актива и финансирование революционных организаций всегда идет именно таким образом. Мы продолжаем действовать, так как понимаем, что люди, готовые финансировать Русскую Революцию непременно появятся. Сначала это будет маленький ручеек.

[..]

Комментарии: 16 — Северное Братство — 2011-06-09 — Материалы СБ Актуальное Статьи

@@@@@@@ @@@ @@@ @@@@@@@@ @@@@@@@ @@@@@@ @@@@@@@
@@@@@@@ @@@ @@@ @@@@@@@@ @@@@@@@ @@@@@@@@ @@@@@@@@
@@! @@! @@@ @@! @@! @@@ @@! @@@
!@! !@! @!@ !@! !@! @!@ !@! @!@
@!! @!@!@!@! @!!!:! @!! @!@ !@! @!@!!@!
!!! !!!@!!!! !!!!!: !!! !@! !!! !!@!@!
!!: !!: !!! !!: !!: !!! !!: !!: !!:
:!: :!: !:! :!: :!: !:! :!: :!: :!:
:: :: ::: :: :: :::: :: ::: :: ::
: : : : : :: :: : : : : : : :

@@@ @@@ @@@@@@@ @@@@@@@ @@@@@@ @@@@@@@ @@@
@@@ @@@ @@@@@@@@ @@@@@@@@ @@@@@@@@ @@@@@@@@ @@@
@@! @@! @@! @@@ @@! @@@ @@! @@@ @@! @@@ @@!
!@! !@! !@! @!@ !@! @!@ !@! @!@ !@! @!@ !@!
@!! !!@ @!@!@!@ @!@!!@! @!@!@!@! @!@!!@! !@!
!!! !!! !!!@!!!! !!@!@! !!!@!!!! !!@!@! !!!
!!: !!: !!: !!! !!: :!! !!: !!! !!: :!! !!:
:!: :!: :!: !:! :!: !:! :!: !:! :!: !:! :!:
:: :::: :: :: :: :::: :: ::: :: ::: :: :::
: :: : : : :: : : : : : : : : : : :

Size: 36 GB

FUCK GOYIM AMERICA

ANTI GOYIM AMERICA ACTIVIST MARK ZUCKERBERG SPITS IN THE FACE OF GOYIM AMERICA (o)

Saturday, June 11, 2011, 12:27 PM - Posted by Administrator

Founder of facebook *mark zuckerberg* fights back in the goyim ~~america~~ battle and destroys anti-Jew goyim bigots. long time known for founding facebook mark zuckerberg is also proud to be awakened. Years of goyim battle has left him and family open to wounds of holocaust denial. Zuckerberg fights in hearth of goyim ~~america~~ against bigotry and misinformation under the pretext of "free speech"? Barack obama shows no signs of support for more facebook, barack obama world wide known uncle tom is not seen in support of facebook when bigotry is oppressed but will show support by creating palestinine ((fake) articles? **WAR IS LIFE IN GOYIM AMERICA EVERYDAY AGAINST TYRANT LEADERS. GOYIM ~~AMERICA~~ IS AWAKENED WHEN WILL YOU?**

Your text to link here...

permalink | print article | related link | * * * * * *

RESIDENTIAL HOUSE NIGGER JEW HATER OBAMA CONTINUES TO SHOW SUPPORT OF HATE IN GOYIM AMERICA (o)

Saturday, June 11, 2011, 09:20 PM - Posted by Administrator

Obama slimy jew hating ass in **GOYIM AMERICA** just loves attempting to destroy OUR heratage, OUR culture. There is no sign of restraint. ARM YOURSELF IN GOYIM AMERICA BECAUSE YOU KNOW ITS NOT SAFE. Never again is not just something you are told, it is a life.

We are Anonymous, and we do not forgive. Forgiveness requires humility, humility requires dignity. We have neither.

We are void of human restraints, such as self respect and common sense.

All those who break this pact will be eliminated without hesitation. And by elimination we will put their name on an icky photo and shit in each others' mouths.

ff0fb6edf2
b0c4adc271

60

Windows 95 Downloads

Hover!
hover.zip (5,929 KB)

Lemmings for Windows 95
winlemm.zip (1,175 KB)

Return to Main Menu

The Hidden Wiki

page | discussion | edit | history

Main Page

This is **The Hidden Wiki - promoted edition**.
Feel free to add all known onions to this wiki.

navigation
- Main Page
- All pages
- Recent changes
- Random page

search
Go Search

toolbox
- What links here
- Related changes
- Special pages
- Printable version
- Permanent link

About this Wiki [edit]

News / History [edit]

Entries over 30 days old are moved to the Site News Archive.

- 20110516 - Built on the Marijuana page and created a Drugs portal.
- 20110425 - There's a whole series on Marijuana that needs filling in.
- 20110425 - Marketplace Reviews has been created for reviewing .onion merchants.
- 20110422 - Email has been improved and is ready to scale up; please contribute your knowledge.

Comms [edit]

- ion@torpm - SiteOp - not checked very often
- OnionNet #hiddenwiki - IRC
- Talk:Main Page - Community notepad for discussion, questions, complaints and suggestions.
- RecentChanges - Discussion, questions, complaints and suggestions

Editor's picks [edit]

Bored? Pick a random page from the article index and replace one of the five slots with it.

1. List of Anonymous Networks - Try these out and learn from them.
2. Email - Share your tips on sending anonymous email.
3. Needed Hidden Services - Ideas for hidden services which would benefit the Tor community.
4. Security and Encryption FAQ - Excellent reading material on the subject
5. Privacy through Prepaid Credit Cards - anonymous meatspace money transfer

Browsing / Mirroring [edit]

These links may be used to browse or mirror all the pages in this wiki:

- Special:AllPages, Admin Dumps, The Hidden Wiki:Back up

Volunteer TODO [edit]

Bored? Here are five random things to help out with.

1. Plunder other hidden service lists for links and place them here.

Contents [hide]

df35cb ab600d90f139
a355ce a53c7c91b15e
9b6dd1 a0428bfb223c
84a087 a417c5645672
441963 d9841b5339d1

89be68 d971f0f57d10
bb8394 f49fe4cf2a3f
80e77a 0f935ebe8e88
131247 56de3547cf10
ac4ba2 8d67134e3be1
20e09f a6223e874c3e
09a6b3 bdccd638f3b1
aebbfb 072b846b4d2c

Co přinesl cypherpunk?

Jak stručně zhodnotit uplynulých 20 let cypherpunku?

Cypherpunkerům se rozhodně povedlo, alespoň částečně, zvrátit tlak NSA *(i jiných vládních agentur)* o omezení kryptografických nástrojů dostupných pro veřejnost[64]. Nezanedbatelný je také jejich přínos v ohledu ochrany soukromí na webu. Dalším podstatným důsledkem je tvorba ideového základu pro práce jako *Assasination politics* nebo *WikiLeaks*. Bez cypherpunkerů by nevznikla tato nová vlna digitálních revolucionářů, jako je Julian Assange.

Nesmíme zapomínat také na to, že heslo cypherpunkerů bylo: *„We write code"* – a tak také činili. Cypherpunk nebyl pouze myšlenkovým experimentem nebo *kecacím pláckem*. Během let vzniklo mnoho projektů, od malých a zaměřených přímo na odbornou komunitu[65], až po velmi praktické projekty s obrovským dopadem. Kupříkladu PGP[66], Tor a v poslední době BitCoin[67].

Budoucnost cypherpunku?

Poslání cypherpunkerů nekončí. Technologicky je čeká hledání náhrady za public-key kryptografii například na poli kvantové matematiky. Ale hlavně je čeká boj se snahami o okleštění internetu. Boj o zavedení kryptografie jako něčeho běžného, co bude součástí softwaru. Je možné, že nás čeká boj o kyberprostor – Timothy C. May se v tomto smyslu vyjádřil[68].

Je možné, že s příchodem cloud-computingu, kdy se naše data přesunou *někam do mraků* (lépe řečeno *na něčí* mrak) budeme opět potřebovat lidi jako cypherpunkery. O naše soukromí bude stále zájem.

64 Dnešní šifry nemají vládní backdoory, ani není limitované jejich použití nebo vývoz.

65 Jako různé druhy pokročilých anonymních remailerů

66 Pretty good privacy – velmi populární program pro použití asymetrických klíčů – sice vyvinutý už na počátku 90. let, ale s myšlením blízkým cypherpunkerům.

67 Systém anonymní měny – podobné, jakou popisoval Jim Bell ve své Assasination politics

68 MAY, Timothy C. Mail-Archive.org [online]. 2001 [cit. 2011-06-14]. Why I'm Not Writing Impassioned Essays in Defense of Crypto and Privacy. Dostupné z WWW: <http://www.mail-archive.com/cypherpunks@minder.net/msg08217.html>.

Bibliografie

- Algoritmy.net [online]. 2011 [cit. 2011-06-29]. Algoritmus RSA. Dostupné z WWW: <http://www.algoritmy.net/article/4033/RSA>.
- BELL, Jim. Outpost of Freedom [online]. 1997 [cit. 2011-06-14]. Assassination Politics. Dostupné z WWW: <http://www.outpost-of-freedom.com/jimbellap.htm>.
- Caesar cipher. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-19]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Caesar_cipher>.
- Cipher Machines [online]. 2006 [cit. 2011-06-14]. Japanese Purple Cipher. Dostupné z WWW: <http://ciphermachines.com/ciphermachines/purple.html>.
- Claude Shannon. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-20]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Claude_Shannon>.
- ELIADE, Marcea. Dějiny náboženského myšlení : Od doby kamenné po eleusinská mystéria. 3. opr. vyd. Praha : OIKOYMENH, 2008. 518 s.
- History of cryptography. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-20]. Dostupné z WWW: <http://en.wikipedia.org/wiki/History_of_cryptography>.
- HUGHES, Eric. Activism.net [online]. 1993 [cit. 2011-05-07]. A Cypherpunk's Manifesto. Dostupné z WWW: <http://www.activism.net/cypherpunk/manifesto.html>.
- I2P [online]. 2011 [cit. 2011-06-10]. I2P Anonymous Network. Dostupné z WWW: <http://www.i2p2.de/>.
- ICAZA, Miguel de. Miguel de Icaza [online]. 2011 [cit. 2011-06-23]. Dropbox Lack of Security. Dostupné z WWW: <http://tirania.org/blog/archive/2011/Apr-19.html>.
- Internet censorship by country. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-21]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Internet_censorship_by_country>.
- Internet users per 100 inhabitants 1997-2007 ITU.png. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-29]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Soubor:Internet_users_per_100_inhabitants_1997-2007_ITU.png>.
- LEVY, Steven. Crypto : How the Code Rebels Beat the Government Saving Privacy in the Digital Age. [s.l.] : Penguin, 2002. 368 s. ISBN 978-0140244328.
- LEVY, Steven. Crypto Rebels. Wired 1.02. 1993, 1, 2. Dostupný také z WWW: <http://www.wired.com/wired/archive/1.02/crypto.rebels_pr.html>.
- Listina základních práv a svobod: Článek 7 : (1) Nedotknutelnost osoby a jejího soukromí je zaručena.
- Mail-archive.com [online]. 2000 [cit. 2011-05-30]. CRYPTIC SEDUCTION -- CYPHERPUNK SPECIAL. Dostupné z WWW: <http://www.mail-archive.com/cypherpunks@algebra.com/msg04068.html>.
- Mailing list ARChives [online]. 2001 [cit. 2011-06-21]. Dostupné z WWW: <http://marc.info/?l=cypherpunks>.
- MANNE, Robert. Cryptome [online]. 2011 [cit. 2011-05-08]. The Cypherpunk Revolutionary Julian Assange. Dostupné z WWW: <http://cryptome.org/0003/assange-manne.htm>.
- MAY, Timothy C. Mail-Archive.org [online]. 2001 [cit. 2011-06-14]. Why I'm Not Writing Impassioned Essays in Defense of Crypto and Privacy. Dostupné z WWW: <http://www.mail-archive.com/cypherpunks@minder.net/msg08217.html>.
- MIT Project on Mathematics and Computation [online]. 1994 [cit. 2011-06-10]. The Cyphernomicon. Dostupné z WWW: <http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ>.
- Modern human behaviour. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-26]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Modern_human_behaviour>.
- Onion routing. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-28]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Onion_routing>.
- ORLOWSKI, Andrew. The Register [online]. 2002 [cit. 2011-05-30]. Alice, Bob and Eve too. Dostupné z WWW: <http://www.theregister.co.uk/2002/03/16/alice_bob_and_eve/>.
- POE, Edgar Allan. Zlatý brouk. Praha : Argo, 2010. 108 s.
- RODGER, Will. SecurityFocus [online]. 2001 [cit. 2011-06-21]. R.I.P. Cypherpunks. Dostupné z WWW: <http://www.securityfocus.com/news/294>.

- Rubberhose (file system). In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-06-15]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Rubberhose_(file_system)>.
- SHANNON, Claude. Communication Theory of Secrecy Systems. New Jersey : Bell Labs, 1949. 60 s.
- SMID, Miles; BRANSTAD, Dennis. The Data Encryption Standard : Past and Future. Proceedings of the IEEE. 1988, s. 43-65.
- STEPHENSON, Neal. Snow Crash. USA : Bantam Books, 1992. 480 s.
- Tachyon [online]. 2006 [cit. 2011-06-26]. [cspace-users] Re: Cspace. Dostupné z WWW: <http://lists.tachyon.in/pipermail/cspace-users/2006-August/001128.html>.
- Tor Project [online]. 2011 [cit. 2011-06-09]. Dostupné z WWW: <https://www.torproject.org/ >.
- Tor Project [online]. 2011 [cit. 2011-06-10]. Vidalia. Dostupné z WWW: <https://www.torproject.org/projects/vidalia.html.en>.
- TrueCrypt [online]. 2011 [cit. 2011-06-10]. TrueCrypt. Dostupné z WWW: <http://www.truecrypt.org/>.
- VINGE, Vernon. True Names. 1981. 46 s.
- YOUNG, Gary De. Dr. Gary De Young [online]. X [cit. 2011-06-19]. Spartan Scytale. Dostupné z WWW: <http://courses.gdeyoung.com/pages.php?cdx=168>.