Beyond Schlock on Screen: Teaching the History of Cryptology Through Media Representations of Secret Communications

Peter Krapp
Professor, Film & Media Studies / Informatics
Humanities Gateway 2321
University of California, Irvine
krapp@uci.edu

Abstract

This paper lays out the course design for, and teaching experiences with, a class that introduces students in the humanities to the history of cryptology, with particular attention to film and media studies. The course covers principles of secret communication from ancient times to the 21st century, and encourages students to develop creative solutions that may help portray computing, computer networks, and cybersecurity issues in more informed and accurate ways on screen.

1 Introduction

While it may seem paradoxical to combine communication and secrecy, in fact media history can be told as the story of secret communications - from long before the earliest radio transmissions and interceptions to long after the commercial union of military technology and entertainment in television. In this course, students discover the media history of codes and ciphers from ancient cultures to the advent of computing, with a focus on secret communication mostly before the proto-computers of Bletchley Park, while connecting historical methods to contemporary questions of secrecy, privacy, and security in the Internet age. Readings include short stories and selected articles and chapters from the history of encryption and code breaking. Each week also features hands-on exercises (in class as well as in homework), and workshops on 21st century applications of historical models, with particular attention to the often fundamentally irreconcilable demands of privacy, security, trust, data integrity, and freedom of speech (Diffie/Landau 2007). This, however, is not a class in computer science or informatics, and it requires neither facility with number theory nor an appetite for algorithms.

The overall arc of the course leads students to ponder the motivations for secure and secret transmissions, from assurances of communication integrity to various forms of authentication, and beyond a naïve identification of concealment with security. Once they wrap their heads around the difference between steganography and cryptology and begin to appreciate the nuances of substitution and transposition ciphers, historical examples from the ancient Skytale to forms of the Pigpen cipher allow hands-on decoding experience. After an aside about steganography and invisible ink, it is time for methods of cracking monoalphabetic substitution (Kahn 1967, Macrakis 2014, Singh 1999). Most students at the University of California have sufficient prior exposure to American history to enjoy exploring secret communications from Independence to the Civil War, amplified by selected screenings from TV shows like *Turn* (2014-2017) about the Culper Ring - which also makes an appearance in season 4, episode 6 (2012-2013) of the TV show *White Collar* in contemporary New York City. Many also enjoy tracing the mechanization of ciphers from the Alberti disc to the Mexican Army disc and from the Jefferson wheel cipher to the US Army's M-94 cylinder used as late as 1942.

Media representations of secrecy and security in communications allow students to tackle the Vigenére table, try taking the Kasiski test, visualize implementations of ciphers from Polybius to ADFGVX, and wrap their heads around Friedman's index of coincidence (Kackman 2005, Bauer 2013). In order to introduce the enduring mystique of Number Stations, it helps to have them listen not just to a few tracks from the CONET Project (1997), but also from the Wilco album *Yankee Hotel Foxtrot* (2001) from a band many of them recognize; moreover, the thriller *Numbers Station* (2013) starring John Cusack and Malin Akerman can lead to a fruitful discussion of how faithful film and

Proceedings of the 2nd International Conference on Historical Cryptology, pages 79-85
Mons, Belgium, 23-26 June, 2019

television should be to real technology. One pivotal homework assignment therefore is a film review focusing on ciphers and codes as they are explored in cinema and television. The list of acceptable titles ranges from *Rendezvous* (1935) and *Cipher Bureau* (1938) to *The Imitation Game* (2014) and *Mr Robot* (2015-2019), but most students tend to pick neither the most recent nor the oldest examples, preferring to stick instead with espionage fare from the eighties or nineties – often several vie for writing up *Sneakers* (1992) or *Pi* (1998).

The course pivots on storytelling and visualization, but since it cannot require advanced mathematics or informatics knowledge, it focuses mainly on ciphers and codes before the advent of computing, without omitting Navajo code talkers, Enigma and Colossus, etc. Students quickly grasp why linguists developed frequency analysis as a way to crack simple substitution ciphers, and how nomenclators and book codes aided trade and diplomacy (Kahn 1967). Yet without requiring students in such a course to tackle prime factorization or hash functions, it is nonetheless important to discuss how much their internet use depends on cryptographic principles – once they share how much their daily life revolves around trust in online communications with banks and stores, doctors and pharmacies, educational institutions and entertainment, it is not difficult to illustrate how much the infrastructure of secure communications depends on asymmetric ciphers (Bauer 2007, Quisquater 1990).

Finally, the course ends with a survey of unsolved cryptological puzzles, touching on Voynich, Beale, Zodiac, and Kryptos (Schmeh 2015, Clemens 2016, Bauer 2017). At the conclusion of this writing-intensive seminar, students are expected to have gained greater facility with the relevant historical and critical vocabulary, deeper knowledge about media history, a keener appreciation for codes and ciphers, an ability to critically evaluate conflicting demands on communication, and a better understanding of both fictional and real secrecy (Glass 2013, Koblitz 2010, Koss 2014). In addition to familiarizing students with conceptual and historical content, this course involves advanced information literacy skills by locating, evaluating and integrating information gathered from multiple sources into discipline-specific writing.

2 Overcoming the schlock paradigm

What does encrypted communication look like? The problem with audiovisual representations of cybersecurity in particular and computer networks in general is that they are all too often turned into ludicrous caricatures on screen. Even computer-focused TV dramas like *CSI: Cyber* (2015) get numerous details so wrong that few computer-literate viewers can stand to watch. Computing is not about blinking lights and pixels - and it does not help to lard the script with misused and mispronounced jargon. Malicious code does not show up in red on your screen, and a forensic review takes more than a few minutes. Cybercrime is more likely to involve phishing for credit card numbers or trade secrets rather than kidnapping. When it comes to real or imaginary risks online, movies and TV shows dish up tired iterations that not only perpetuate stereotypes of hacking as (usually male) teenage flirtation with crime, but perhaps offend even more in how they depict data 'space' as an arcade game.

The countless TV shows and movies that get computing, encryption, and decryption wrong tend to make two types of mistakes: they want to glamorize the actions of a person in front of a computer, and they try to visualize the flow of data in networks, often in a ludicrous manner. Take the recent Michael Mann movie *Blackhat* (2015), which has Chris Hemsworth's character come out of prison to help combat international cybercrime. Setting aside the idea that Thor should be a computer nerd (and that he reads Baudrillard and Derrida in his prison cell instead of, say, Schneier or Kahn), while the plot features tricking a government employee into changing his password (so an outsider may gain access), its garish attempt to visualize data on a network is a major throwback to the bad old days of films like *The Net* (1995), *Hackers* (1995), *Sneakers* (1992), *War Games* (1983), or *Tron* (1982). Of course, *Hackers* (1995) is remembered mainly because it featured Angelina Jolie as one of two high schoolers involved in corporate extortion, but it also featured a virus that can speak and has a face, and its protagonists spend more time trash talking and partying than using computers. *The Net* (1995) has Sandra Bullock stumble around bulletin boards as if ordering pizza online was a radical act of subversion, and while this film does show some true aspects of the net (such as IP addresses), it does not do enough with them to ground it in computing reality - you could not connect via telnet to an email address, for instance, you need an IP address and a TCP port number: only once you are connected can you initiate an email login. Nor would a Macintosh virus from 1995 infect a mainframe computer.

Interestingly, *Sneakers* (1992), an ensemble caper conceived during the making of *Wargames* (1983), features a black box capable of breaking any and all computer encryption, threatening to destabilize the world economy (which already raises the issue of post-quantum cryptography). Both movies tend to play fast and loose with computer technology - while you may be able to change your high school grades from a home computer if your school is sloppy, you most definitely won't be able to launch ICBMs with the same machine over the same dial-up modem. *Tron* (1982) is venerable for its pioneering use of computer graphics, but the idea that you can enter the network and act there as if it was a wireframe videogame has had a pernicious influence on film and television.

But perhaps one of the funniest transgressions against computing in a movie is *Swordfish* (2001), a Travolta extravaganza that sees Hugh Jackman's character forced to remotely access a computer of the Department of Defense (via an ancient PDP10 in a CalTech basement), which the actor does by typing really fast and clapping his hands while being threatened by thugs and at the same time sexually engaged by a young woman... and of course he pulls it off within 85 seconds, despite having suffered a long-term ban from using computers; and of course his old software, extant in some basement on tape, may look like vintage graphics software but it acts like a destructive worm... At least in *Superman III* (1983), Richard Pryor's character was allowed to concentrate on hacking a weather satellite, as unlikely as it is that you would do that in BASIC with some PRINT and LIST commands - let alone change payroll data, mess with traffic lights, and other exploits of Pryor's role as a recent computing acolyte.

Yet sadly, things have not become much more sophisticated over the years - consider, for instance, the recent TV show *Homeland* (2011-2019): who believes that the CIA server two Berlin-based online activists accidentally chance upon (in the fifth season, 2015) would grant them access to a directory full of files whose inordinately long names all contain the character string CIA? Do all your file listings contain your employer's name? We are supposed to believe that pulling a physical cable out of the wall is the only thing experts in Langley can do to defend the CIA against an onslaught of internet connections seeking pornographic cam-shows? Shows like that tend to take computers less seriously than Indiana Jones is serious about archeology...

This is not just a question of verisimilitude or realism. While sci-fi author Arthur Clarke stipulated that “Any sufficiently advanced technology is indistinguishable from magic,” this relies on a notion of widespread ignorance that is a legacy of pre-literate times and incompatible with the aims of education. Magic may be acceptable in fantasy fiction but not at university; we are interested in applicable concepts. So a student who wants to discuss Harry Potter in this class should consider two-factor authentication - the combination of something you have (e.g. a wand) or something you are (not a “muggle”) and something you know (a passphrase) for common-room access at Hogwarts; not to mention parseltongue access to the Chamber of Secrets, or maybe the “blood password” needed to access the Horcrux Cave... How can films portray restricted access to The Leaky Cauldron, to Diagon Alley, and to Platform 9 3/4 at King's Cross? Who has access (and how) to the prefects' bathroom or to Dumbledore's office? These questions may seem fanciful, but the stakes are very real.

Before the recent TV show *Mr Robot* (2015-2019), television did not often show computer security issues in a realistic light. But *Mr Robot* is a show that pivots on the activities inside a cyber-security firm, the code it displays on computer screens is real, and there are no hokey sound effects or flights of fancy. Even the hack on this show of an android phone, by inserting a chip that runs a bootloader, is a reference to realistic technology, in this instance the Flexispy software. Remarkably, *Mr Robot* does not shy away from discussing TOR routers, a distributed denial of service attack on corporate servers, and getting people to install malware - in this case, a remote access trojan that resembles an actual piece of software called DarkComet.

Ironically, the sci-fi conspiracy pastiche of *The Matrix Reloaded* (2003) is one of the few movies in the entire schlock genre to show a realistic scene: eschewing for once the usual antics of visualizing cyberspace as a vertiginous flight through the dim canyons of some badly rendered

Data-Manhattan, the movie shows Trinity (neither male nor a teen, but played by Carrie-Anne Moss), working at a keyboard instead of some futuristic interface contraption, using an actual piece of software to scan a power grid for weaknesses: NMAP, a port scanner on the command line, known to system administrators around the world. The German cyber-thriller *Who am I? No System is Safe* (2014) features a similar presentation of software exploits on the power grid – protagonist Benjamin seeks to remotely compromise a local utility using a script that seems to be endowed with universal powers in a command shell. In the thriller *The Bourne Ultimatum* (2007), the CIA hacks the mail server of a British newspaper, and the screen shows the realistic use of SSH, Postfix SMTP, and a domain name server in a UNIX shell. Another franchise thriller from the same year featured an interesting exploit within the first ten minutes: *Live Free or Die Hard* (2007) had its protagonist team up with a young hacker to fight a cyberterrorist. Meanwhile, the Swedish cinematic adaptation of the Stieg Larson book *The Girl with the Dragon Tattoo* (2009) shows her computer skills, again right in the first ten minutes, while the Hollywood remake (2011) does not. At least in the superhero flick *Fantastic Four* (2015, based on the Marvel Comics), you can see Sue Storm (played by Kate Mara) tracking down a companion online: her screen flashes "IPSCAN", "TRACEROUTE" and "PORTSCAN" - it is all too rare to see actual network technology represented.

Of course, getting computer technology right on screen is not just about software and hardware; cybersecurity is also about social engineering – the exploitation of patterns of behavior, vulnerabilities and opportunities. While hardware manufacturers clearly work closely with film and television producers to show off their wares, the software industry and the educational sector both miss out on opportunities to show computing as interesting, stimulating, and challenging - without faking it. Indeed, popular culture no longer celebrates hacking as the generally innocuous but occasionally very profitable pursuit of the computer hobbyist. Television stopped romanticizing the obsessions of talented nerds, the press no longer touts the bootstrapping spirit of digital capitalism. Instead, journalists are busy selling the sinister specter of hacking as an irreducible systemic threat of digital media. Never mind that until the late 1980s, a hacker was someone who, by trial and error and without referring to any manuals, ended up successfully operating computers. Only a few years later, commentators already began to fret that malicious hacking might pose a serious and costly problem. For the longest time, digital culture had focused on access, learning, privacy, and free speech (Bamford 1982, Levy 2001, Schneier 2004). Yet in a sea change in popular opinion as well as legal and economic policy regarding network technology and education, alarmist commentators began to demonize anyone who tried to access more than the official, limited interface allowed.

3 Assignment Design

A cult of secrecy can easily lead to a global resurgence of irrational rumor, and unfortunately this is indeed what one sees in a lot of internet culture. When conspiracy theory takes the place of critical computer culture, our future is seriously impoverished. Arguably, teaching students in film and media studies about basic concepts of cybersecurity, and getting them interested in the outlines of the history of cryptology, may in time greatly increase the chances for scripts and scenes that provide more accurate and more intelligent audiovisual representations of computing and of communication security.

In order to heighten attention to both the problematic audiovisual representation of cybersecurity as well as to the possibilities of visualizing cryptology in persuasive and plausible ways, students are tasked with writing synoptic treatments for films or TV pilots based on assigned short stories. While a synopsis is different from a full treatment in industry parlance (a synopsis distils the narrative into a brief pitch, while a treatment gets into nuts and bolts of representing a story audio-visually), for the pedagogical purposes of this course, what is solicited is a document that highlights the necessary details with some cinematic style and rhythm, giving a feeling for characters, mood, and visual settings evocative of a time and place. Such a synoptic treatment is not simply a retelling of the story; it should be a document that might allow a decision-maker to evaluate the idea as well as its intended audiovisual execution. Marking story beats with particular attention to how to present issues of secret communication on screen, it needs to include a title and logline, introduce major characters, set the scene, dramatize the main conflicts leading to a crisis, and envision the dramatic resolution. Unlike a short story, the synoptic treatment cannot tell us a character's thoughts but needs to show them, it cannot provide background but needs to outline dialogue; for pedagogical reasons (and because writing actual dialogue is hard), the task here is to succinctly describe the dialogue that a fully-fledged screenplay would provide. The short stories assigned were culled mostly from American and British detective fiction dating to the turn of the 20th century. In turning such old-fashioned material into a synoptic treatment, students are not simply retelling a piece of fiction, but updating and retooling its story beats to suit their own contemporary taste, with particular attention to how one can present secret communications on screen.

In addition, students compile reference materials resembling 'encyclopedia entries' about certain names and concepts that are important to the history of cryptology. Here the task is to conduct some research (a minimum of 4-5 references), define/describe/discuss what the keyword denotes or who the person is/was, and how exactly this entry relates to course topics. At least one reference source must be drawn from an online database for academic research (such as JSTOR or Project MUSE) in order to familiarize students with library systems for academic work. With names ranging from Alberti and Trithemius to Diffie and Schneier, and concepts including Kerkhoff's Principles, a Zero Knowledge Proof, Atbash, PGP, or the Clipper Chip, students sometimes struggle to fit all their findings into an encyclopedia entry that is concise yet comprehensive in scope.

An in-class midterm mixes multiple choice questions about historical facts with a few open-ended prompts that solicit a few paragraphs of reflection. How do you use a keyword to enhance the Caesar cipher? What is the second most common trigram in English? What kinds of sympathetic stains can you list? What was the name for the ancient Greek method to secure confidential messages? Which early US diplomat is associated with a wheel cipher? What is the first step to begin cracking a message if you know it was enciphered with the Vigenère method but you do not have the key? What led Babbage to a statistical breakthrough in cryptanalysis, and why did he not publish it, but Kasiski later did? A final take-home essay on a research topic directly related to course materials is expected to be more substantial, and again at least one source must be drawn from an online database for academic research (such as JSTOR or Project MUSE), and the individual research topics and essay drafts are workshopped in class. Should governments be able to access anyone's encrypted communication to prevents crimes, or should technology companies deploy encryption as unbreakable as possible to protect widespread privacy and security? What are contemporary forms of steganography, and how practical does it seem to store and/or transmit secret information in superficially unaltered sound files, images, videos, etc.? As with all assigned writing, both in class and at home, students provide peer review on multiple drafts though a shared course portal, so that graded assignments are never first drafts with all their usual flaws.

4 Feedback

Students quickly find out for themselves why the depiction of secret communications on screen is often so stilted and wrong-headed, but a few found rather creative solutions that their peers justifiably celebrated in peer-review sessions. Unlike the analytic and critical mode university students in the humanities are commonly expected to exercise, many of these assignments are not explanations or comments on what they read. If your writing must prepare for telling a story with audiovisual means, you are neither spelling out a character's thoughts, nor providing biographical or technical background. Granted, one must not expect truly creative writing – students know that they should neither copy nor invent dialogue or characters for their synoptic treatments. Once they see that they can remain faithful to the conceptual dimensions of each short story and yet put considerable inventiveness into the pitch for a screenplay based on it, they deliver with impressive ingenuity.

On the other hand, even if they enjoy puzzling out how to write their own names in Pigpen, or how best to define the differences between substitution and transposition ciphers, one should not expect humanities students to install JCrypt on their computers, or to study the math involved in public key crypto (Koblitz 1997, Kaur 2008, Winkel 2008, Kurt 2010). But one certainly can expect them to work through a curriculum that surveys the history of secret communication, albeit mostly pre-computing, and draw conclusions for their own lives in the 21st century. Even or especially if they are not budding computer scientists, they need to be able to debate the role of cryptography during World War II, reading about Enigma and Purple, about Alan Turing and the Polish mathematicians who made seminal discoveries. Students invariably show themselves engaged with current cybersecurity, from password management to the trust they put in various communication platforms, whether WhatsApp or Messenger or Telegram or Signal. They tend to be enthusiastic about social media, and generally much less skeptical about data mining and advertising than national surveys suggest they might be (Pew Research Center 2018). They not only get a kick out of the Zimmerman Telegram, but even more so out of imagining its contemporary equivalent as a *casus belli.* They tend to be rather skeptical about some of David Kahn's claims about why the Germans lost to US intelligence in World War II; they neither vilify nor venerate characters like Julian Assange or Edward Snowden, and their discussions and homework show a clear preference for discussing the security of gaming servers over that of credit card companies, or whether to trust social media platforms rather than political institutions.

Students tend to have animated and well-informed discussions of the stakes of online identity, anonymity, and pseudonyms. They never acquiesce to a majority viewpoint, though, and some maintain reservations throughout the entire course about certain conflicts between privacy and public security, trust and advanced technology, freedom of speech and personal accountability online.

Writing synoptic treatments that seek to update classic detective fiction like the Sherlock Holmes yarn about the Dancing Men or an Isaac Asimov short story about encryption, students show ingenuity in visualizing a code that might be like graffiti, hidden in plain sight. Perhaps not surprisingly given that they are less likely to own printed books and more likely to read digital files on their various devices, fewer students become interested in book codes, as featured in season two of the TV show *Burn Notice* (a stolen bible dominates the entire season's plot, 2008-2009), in the movie *National Treasure* (where coordinates on the back of the Declaration of Independence lead to elusive treasure, 2004), or in the Sherlock Holmes mystery *The Valley of Fear* (1915), despite the enduring popularity of Holmes as a character on TV and on the big screen. Also perhaps unsurprisingly, students tend to be less interested in codes that involve more than one language, even though they appreciate that the history of cryptology for a long time was entwined with translation and philology, and not only in prominent ways like the Rosetta Stone or in decoding German and Japanese World War II communications.

By the same token, students tend to show a refreshing lack of respect for old-fashioned aspects of the short stories they were tasked to update; instead of snuff boxes, poisoned pens, and handkerchiefs, their versions of these stories feature smartphones, dance clubs and graffiti, and rather than see their characters scandalized by allegations of infidelity or fiscal impropriety, their envisioned plots twists include social media gaffes and wet t-shirt contests. In the end, the aims of the course are demonstrably achieved, as evident in the students' confident command of historical and conceptual dimensions of cryptology in their final essays. There are usually quite a few essays on questions of identity theft and how to protect oneself against it. There are usually competent arguments for, as well as against, government access to encryption backdoors; some ambitious and more computer-literate students are also game to puzzle over unsolved ciphers (Schmeh 2015, Bauer 2017), or to tackle the task of demonstrating how Auguste Kerckhoffs' principles (from 1883) are still valid in today's mobile media culture.

Students also enjoy a brief weekly exercise that introduces various technical implementations of the issues studied in the class, from the proper set up of browsers and virtual private networks to comparing password managers, from multi-factor authentication to safe use of social media. Now that the university they enrolled with is moving to systems that require multi-factor authentication, they see that passwords alone are no longer sufficient in preventing unauthorized access of individual and institutional resources; and most students turn out to be rather passionate about protecting their personally identifying information. Since passwords, even in the academic environment, are now routinely compromised through malware, brute force attacks, phishing, and other exploits, the history and future of secure communication raises new questions that are directly relevant to their everyday lives. Part of the impact of this course is to lead students to discover basic principles for themselves, instead of nudging their behavior as institutions tend to try.

Integrating online resources into the course has also greatly aided the contextualization. An Instagram account is a more readily accessible repository of images from the history of cryptography than slides used to be. Students can see on the calendar of the National Cryptologic Museum Foundation what happened on this day in cryptologic history, they can use morse coders and decoders, play with Pigpen fonts and anagram servers, and cast a far more informed look at the cyber security training resources of the university. Several times, I teamed up with IT specialists on campus responsible for propagating safe online behavior among students, and whether it was screenings and discussions or more focused panel presentations, the students who had taken this class did far better on the Cybersecurity training modules of the university than the general public does according to relevant surveys (Pew Research Center Cybersecurity Knowledge Quiz, 2017).

Acknowledgments

I thank the students in my writing seminars on the media history of secret communications at the University of California, Irvine in 2005, 2011, 2017, and 2019.

References

James Bamford. 1982. *The Puzzle Palace: Inside the National Security Agency.* Penguin, New York.

Craig P Bauer. 2013. *Secret History: The Story of Cryptology.* CRC Taylor & Francis, Boca Raton.

Craig P Bauer. 2017. *Unsolved! The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies.* Princeton University Press, Princeton NJ.

Friedrich L Bauer. 2007. *Decrypted Secrets: Methods and Maxims of Cryptology.* Springer, Berlin.

Raymond Clemens. 2016. *The Voynich Manuscript.* Yale University Press, Yale CT.

Whitfield Diffie and Susan Landau, 2007. *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press, Cambridge MA.

Darren Glass. 2013. "A First-Year Seminar on Cryptography", *Cryptologia*, 37:4, 305-310

David Kahn. 1967. *The Codebreakers – The Story of Secret Writing.* Macmillan, New York.

Michael Kackman. 2005. *Citizen Spy: Television, Espionage, and Cold War Culture.* University of Minnesota Press, Minneapolis.

Manmohan Kaur. 2008. "Cryptography as a Pedagogical Tool", PRIMUS v18 n2 (March 2008), 198-206

Neal Koblitz. 1997. "Cryptography as a Teaching Tool," *Cryptologia* 21:317–326.

Neal Koblitz, 2010. "Secret Codes and Online Security: A Seminar for Entering Students," *Cryptologia*, 34:145–154

Lorelei Koss. 2014. "Writing and Information Literacy in a Cryptology First-Year Seminar," *Cryptologia* 38:223-231

Yesem Kurt. 2010. Deciphering an Undergraduate Cryptology Course, *Cryptologia*, 34:2, 155-162

Stephen Levy. 2001. *Crypto.* Penguin Books, London

Kirstie Macrakis. 2014. *Prisoners, Lovers, and Spies: The Story of Invisible Ink from Herodotus to al-Qaeda.* Yale University Press, Yale CT.

National Cryptologic Museum Foundation. https://cryptologicfoundation.org

Pew Research Center: Americans and Cybersecurity https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

Pew Research Center Cybersecurity Quiz, 2017 https://www.pewinternet.org/quiz/cybersecurity-knowledge/

Klaus Schmeh. 2015. List of Encrypted Books. http://scienceblogs.de/klausis-krypto-kolumne/klaus-schmehs-list-of-encrypted-books/

Simon Singh. 1999. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* Anchor Books, New York.

Bruce Schneier. 2004. *Secrets and Lies. Digital Security in a Networked World.* Wiley, Indianapolis.

Jean-Jacques Quisquater et al. 1990. "How to Explain Zero-Knowledge Protocols to your Children", in G Brassard ed., *Advances in Cryptology – Crypto 89.* LNCS 435, pp 628-631.

Brian Winkel. 2008. Lessons Learned from a Mathematical Cryptology Course, *Cryptologia*, 32:1, 45-55