Krapp, Peter. Comunicação secreta e história da criptologia: um desafio para as Humanidades Digitais. *TECCOGS* – Revista Digital de Tecnologias Cognitivas, n. 21, jan./jun. 2020, p. 146-165. Tradução de Eduardo Harry Luersen.

Recebido em: 01 fev. 2020
Aprovado em: 27 fev. 2020

dx.doi.org/
10.23925/1984-3585.2020i21p146-165

Comunicação secreta e história da criptologia: um desafio para as Humanidades Digitais

Peter Krapp[1]

Tradução do inglês: Eduardo Harry Luersen

Resumo: Estudar a comunicação sob a perspectiva do sigilo soa paradoxal. Entretanto, pode-se afirmar seguramente que guardar é tão importante quanto compartilhar. Durante séculos a história da criptologia remeteu aos campos da linguagem, da tradução, da escrita e da interpretação, porém, desde a década de 1940 ela tem se baseado cada vez mais na matemática e na computação. No século xxi, a cultura digital depende da encriptação para que os sujeitos se comuniquem de maneira confiável e verificável com seus bancos, médicos, advogados e parceiros de negócios. Confrontar a questão da encriptação na atualidade demanda uma análise crítica das suas representações deturpadas. Indicamos que estamos trabalhando com Humanidades Digitais ao aplicarmos métodos das ciências de dados à comunicação estética. Então por que não o fazemos também quando aplicamos métodos das Ciências Humanas para pesquisar a cultura digital? Apesar de Galloway nos advertir que, na tarefa de processar e analisar informação quantitativa, "um pesquisador do campo da cultura que empregue tais métodos é pouco mais do que uma versão inferior da Amazon ou da Equifax", é preciso que as Humanidades Digitais ajudem a reduzir a distância entre as abordagens quantitativas e qualitativas. Este artigo apresenta o projeto de um programa de ensino e a experiência pedagógica com uma turma de alunos de Ciências Humanas sobre a história da criptologia. Abordando a comunicação secreta desde tempos remotos até os dias de hoje, o artigo também explora como as mídias retratam as redes de computadores e como abordam o tema da cibersegurança.

Palavras-chave: Sigilo. Encriptação. Criptoanálise. Cibersegurança. Deturpações.

1 Professor e coordenador do Departamento de Estudos de Cinema e Mídias na Universidade da Califórnia, em Irvine. Lecionou na Universidade de Minnesota e na Bard College e foi Pesquisador Visitante em Universidades na África do Sul, Alemanha, Brasil, Estados Unidos e Taiwan. É autor dos livros *Déjà Vu: Aberrations of Cultural Memory* (2004) e *Noise Channels: Glitch and Error in Digital Culture* (2011).

Secret communication and cryptologic history: a challenge for digital humanities

Abstract: It may seem paradoxical to study communication from the vantage point of secrecy, but arguably keeping is as important as sharing. For centuries, cryptologic history was about languages and translation, writing and interpretation, though since the 1940s it relies much more on math and computing. Digital culture in the 21st century relies on encryption for trustworthy and verifiable communications among people and their banks, doctors, lawyers, business partners. Addressing the stakes of encryption today requires a critical appreciation of its misrepresentations - digital humanities are invoked when we apply data-science methods to aesthetic communication, so why not when we apply Humanities methods to digital culture? Despite Galloway's warning that in parsing and processing quantitative information, "a cultural worker who deploys such methods is little more than a lesser Amazon or a lesser Equifax", digital humanities need to help bridge the gulf between quantitative and qualitative approaches. 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. Covering secret communication from ancient times to today, the paper also surveys how media portray computer networks and cybersecurity issues.

Keywords: Secrecy. Encryption. Cryptanalysis. Cybersecurity. Misrepresentation.

A história das mídias pode ser contada como a história das comunicações secretas – desde muito antes das primeiras transmissões de rádio e das suas interceptações, até muito depois da televisão, que uniu comercialmente a tecnologia militar ao entretenimento[2]. Restam poucas dúvidas de que a cultura digital carrega, por todos os lados, as marcas dos debates sobre encriptação, segurança e confiança da comunicação entre os sujeitos e seus bancos, médicos, advogados e parceiros de negócios. Além disso, quando aqueles que se opõem a uma comunicação mais segura apelam a falácias sobre o "lado sombrio" da comunicação mediada por computadores, é preciso que enfrentemos o tema da encriptação partindo de uma análise crítica das suas representações deturpadas[3].

As Humanidades Digitais não precisam implementar um uso estrito de ferramentas das chamadas ciências de dados para explorar as dimensões quantitativas dos seus objetos de interesse tradicionais; é perfeitamente possível utilizar uma abordagem interpretativa e manter a conversação das Humanidades Digitais com as Humanidades propriamente ditas. Na medida em que os mecanismos de busca prometem acesso em tempo real aos acervos das bibliotecas de pesquisa, em que as editoras acadêmicas se voltam à distribuição online e que instituições como a Biblioteca do Congresso Norte-Americano postam suas coleções na internet, os computadores passam a fazer parte do ensino e da curadoria da literatura, da história e da cultura audiovisual. A textualidade digital tem sido celebrada como uma nova forma de literatura, uma nova enciclopédia, uma biblioteca universal e como um metameio capaz de ingerir e substituir as mídias anteriores – mas também surgem novos formatos audiovisuais, que mobilizam nossa atenção a partir de modos de narração e interação distintos. A introdução da questão tecnológica nas Ciências Humanas altera o foco para as redes de tecnologias e instituições que per-

2 Este artigo é uma versão atualizada e traduzida de uma publicação anterior: Krapp, Peter. Beyond schlock on screen: teaching the history of cryptology through media representations of secret communications. *Proceedings of the 2nd International Conference on Historical Cryptology* (HistoCrypt 2019), Linköping University Electronic Press, NEALT Proceedings Series 158:009, p. 79-85. Disponível em: <ep.liu.se/ecp/contents.asp?issue=158>. Acesso em: 25 mar. 2020.

3 Agradeço aos alunos dos meus seminários de escrita sobre a história das mídias da comunicação secreta da Universidade da Califórnia, em Irvine, das turmas de 2005, 2011, 2017 e 2019.

mitem que uma determinada cultura escolha, armazene e processe dados importantes. Também nos convida a explorar as frestas entre as práticas acadêmicas, como na suplementação dos modelos espaciais (texto, grafismos, ilustrações) com modelagens temporais destes dados (vídeos, modelos interativos), por exemplo. Ainda assim, há aqueles que entendem que a maioria das práticas das Humanidades Digitais não são propriamente Ciências Humanas. Para abrandar tais inquietações, as Humanidades Digitais devem construir formas de aplicar os métodos das Ciências Humanas à cultura digital, e não apenas utilizar as ferramentas digitais para exibir e representar temáticas tradicionais das Humanidades.

Podemos ilustrar esta controvérsia a partir de uma pesquisa sobre a comunicação secreta desde os tempos remotos até hoje. Esta costumava ser uma competência fundamental das Ciências Humanas: durante séculos, a história da criptologia se ocupou das linguagens e suas traduções e da escrita e sua interpretação. Evidentemente, desde a década de 1940 ela tem sido cada vez mais baseada na computação e na matemática – mas isto não significa que devamos abandonar completamente o tema aos engenheiros de software e teóricos dos números. Apesar de Galloway (2014, p. 110) nos advertir que, na tarefa de processar e analisar informação quantitativa, "um pesquisador do campo da cultura que empregue tais métodos é pouco mais do que uma versão inferior da Amazon ou da Equifax", é preciso que as Humanidades Digitais ajudem a reduzir o abismo existente entre as abordagens quantitativas e qualitativas. Para testar a minha hipótese de que tanto a história como o atual debate sobre a segurança e a confiabilidade da informação seguem sendo preocupações fundamentais das Ciências Humanas, e que uma competência em Humanidades Digitais pode ser muito importante a esta dimensão, projetei e lecionei um curso que rastreia a longa história das comunicações secretas, e que simultaneamente extrapola, a partir de articulações históricas, diversas questões sobre a vida diante das condições técnico-midiáticas do século XXI.

Neste curso, os alunos desvendam uma história das mídias dos códigos e criptogramas de culturas remotas até o advento da computação, concentrando-se na comunicação secreta ainda anterior aos proto-computadores de Bletchey Park, e conectando os métodos históricos a questões contemporâneas sobre sigilo, privacidade e segurança na era da internet. A bibliografia inclui contos, artigos selecionados e capítulos de livros sobre a história da encriptação e da quebra de códigos. A cada semana também são realizados exercícios práticos (em sala de aula e lições de casa) e oficinas sobre aplicações contemporâneas de modelos históricos, com uma atenção particular aos apelos, na maioria das vezes essencialmente

inconciliáveis, por privacidade, segurança, confiança, integridade de dados e liberdade de expressão (Diffie e Landau, 2007). Todavia, por não se tratar de um curso de Ciências da Computação ou de Informática, não se demanda que os estudantes saibam trabalhar com aritmética ou que nutram um interesse pelos algoritmos. O arco geral do curso leva os alunos a considerarem as motivações de uma transmissão sigilosa e segura, que vão desde as garantias de integridade da comunicação às suas várias formas de autenticação. Isto permite contornar o equívoco ingênuo de se tomar ocultação e segurança como sinônimos. Uma vez tendo compreendido a diferença entre esteganografia e criptologia, as nuances entre as cifras de substituição e de transposição, os alunos estão aptos a realizar experiências práticas de decodificação a partir de exemplos históricos que vão desde a antiga cítala até a cifra maçônica. Após uma digressão sobre a esteganografia e a tinta invisível, é possível explorar os métodos de decodificação das cifras de substituição monoalfabética (Kahn, 1967; Macrakis, 2014; Singh, 1999). A maior parte dos alunos da Universidade da Califórnia tem uma exposição anterior suficiente à história dos Estados Unidos, de modo que se torna interessante explorar as comunicações secretas da Guerra de Independência à Guerra Civil. Esta experiência é amplificada pela mostra de episódios selecionados de séries televisivas como *Turn* (2014-2017), sobre o *Culper Ring*[4] – que também aparece no sexto episódio da quarta temporada (2012-2013) da série *White Collar: Crimes do Colarinho Branco*, ambientada na Nova Iorque contemporânea. Muitos alunos gostam de rastrear os processos de mecanização das cifras, desde o disco de Alberti até o disco do exército mexicano ou do disco de Jefferson ao cilindro M-94, utilizado pelo exército dos EUA até 1942.

As representações midiáticas do sigilo e da segurança da comunicação permitem que os alunos explorem a cifra de Vigenère, tentem observar o método Kasiki, visualizem as implementações de cifragens desde o quadrado de Políbio até a cifra ADFGVX e compreendam o índice de coincidência de Friedman (Kackman, 2005; Bauer, 2013). Para introduzi-los à mística indelével das chamadas emissoras de números, eles escutam não apenas as gravações do Projeto CONET (1997), mas também ao álbum *Yankee Hotel Foxtrot* (2001) da banda Wilco, com a qual já têm certa familiaridade; além disso, o thriller *Códigos de Defesa* (2013), estrelado por John Cusack e Malin Akerman, conduz a uma produtiva discussão sobre o quão fiel às tecnologias reais o cinema e a televisão deveriam ser.

4 Nota do tradutor (N.T.): o *Culper Ring* foi uma organização de espiões gerenciada pelo major Benjamin Tallmadge durante a ocupação britânica da cidade de Nova York, no apogeu da Guerra de Independência dos Estados Unidos (1775-1983).

Figura 1: Objetos de comunicação secreta apresentados na série *Turn*. Fonte: AMC. Disponível em: <amc.com/shows/turn/season-1>. Acesso em: 6 abr. 2020.

Figura 2: As emissoras de números representadas em *Códigos de Defesa*. Fonte: *HFUnderground*. Disponível em: <hfunderground.com/wiki/Numbers_stations_in_popular_culture>. Acesso em: 6 abr. 2020.

Em razão disso, um dos trabalhos de casa indispensáveis do curso é a escrita de uma resenha crítica sobre um audiovisual, enfatizando como as cifras e os códigos são retratados no cinema e na televisão. A lista de audiovisuais aceitáveis para este trabalho compreende obras que vão desde *Um Tenente Amoroso* (1935) e *Cipher Bureau* (1938) até *O Jogo da Imitação* (2014) e *Mr. Robot* (2015-2019). Porém, a maioria dos alunos não costuma escolher os exemplos mais antigos nem os mais recentes, optando seguidamente por filmes de espionagem dos anos 1980 ou 1990, como *Quebra de Sigilo* (1992) e *Pi* (1998).

O curso trabalha com narrativas e suas visualidades e, como não requer conhecimentos avançados de matemática nem de informática, explora principalmente aquelas cifras e códigos anteriores ao advento da computação, sem excluir os códigos *Navajo*, a máquina *Enigma*, o computador *Colossus*, dentre outros. Os alunos logo entendem porque os linguistas desenvolveram a análise de frequências como uma forma para decodificar cifras de substituição simples, e como os nomencladores e os livros de códigos auxiliaram no comércio e na diplomacia (Kahn, 1967). Por não exigir que os alunos do curso saibam realizar fatoração primária ou funções de dispersão criptográfica (funções *hash*), é de fundamental importância fomentar discussões sobre como o seu uso da internet é dependente de princípios criptográficos – uma vez que eles tenham partilhado o quanto as suas vidas cotidianas estão em torno da confiança nas comunicações online com bancos e lojas, médicos e farmácias, instituições educacionais e formas de entretenimento, fica fácil ilustrar o quanto a infraestrutura da segurança das comunicações depende de criptogramas assimétricos (Bauer, 2007; Quisquater, 1990).

O curso é concluído com um exame de quebra-cabeças criptológicos sem resolução, abordando o Manuscrito Voynich, as cifras de Beale, o enigma do Zodíaco e o *Kryptos* (Clemens, 2016; Bauer, 2017; Schmeh, 2015). Ao terminarem este seminário de escrita intensiva, espera-se que os alunos tenham desenvolvido: um vocabulário crítico e histórico relevante; um conhecimento mais aprofundado sobre a história das mídias; uma apreciação mais perspicaz dos códigos e criptogramas; a habilidade para analisar criticamente as reivindicações conflitantes sobre a comunicação; e um melhor entendimento do sigilo ficcional e real (Glass, 2013; Koblitz, 2010; Koss, 2014). Além de familiarizar os alunos a conteúdos conceituais e históricos, este curso envolve o desenvolvimento de habilidades avançadas de literacidade da informação, a partir da procura, avaliação e integração de informações de fontes diversificadas para a escrita específica exigida pela disciplina. Ainda assim, a principal dificuldade de um curso como este se trata de como superar o paradigma do *schlock* – o fato irrefutável de que a maioria das representações midiáticas das comunicações secretas são batidas, estereotípicas, deturpadas, enganosas ou simplesmente erradas. É sob este aspecto que a exposição ao uso prático e experimental das ferramentas digitais se torna uma necessidade pedagógica.

Qual é a aparência da comunicação encriptada? O problema com as representações audiovisuais da cibersegurança, em particular, e das redes de computadores, em geral, é que com grande frequência elas são transformadas, na tela, em caricaturas extravagantes. Mesmo as séries televi-

sivas em que a computação é central, como *CSI Cyber* (2015), interpretam inúmeros detalhes de forma tão equivocada que são poucos os telespectadores com alguma experiência em informática que aguentam assisti-las. A computação não se trata de pixels e luzes piscando – e em nada ajuda inundar o roteiro com um jargão mal utilizado e pronunciado. Os códigos nocivos não piscam em vermelho na sua tela, e uma análise forense da máquina demora mais do que alguns minutos. Em sua maior proporção, os cibercrimes se ocupam do "*phishing*" de números de cartões de crédito e de segredos comerciais, e apenas muito raramente de sequestros. Ao tratarem dos riscos online reais e imaginários, os filmes e as séries de TV costumam entregar repetições desgastadas, que são nocivas não apenas por perpetuarem os estereótipos do *hacking* como um flerte adolescente (e normalmente masculino) com o crime, como também por representarem a forma do "espaço" de dados como se fosse um jogo de fliperama.

Mesmo que este seja um problema global, meus exemplos audiovisuais têm um viés anglófono e centram-se nos EUA; mas poderíamos substituí-los por exemplos vindos de muitos outros lugares. Os incontáveis filmes e séries norte-americanos que se equivocam quanto à computação, encriptação e decriptação, tendem a cometer sobretudo dois tipos de erros: a glamorização das ações de uma pessoa em frente a um computador e a tentativa de tornar visível o fluxo de dados em rede, normalmente de maneiras extravagantes. Tomemos como um exemplo inicial o filme *Hacker* (2015), de Michael Mann. Nele, a personagem de Chris Hemsworth sai da cadeia para ajudar no combate internacional ao cibercrime. Ignoremos a ideia de que o Thor deveria ser um nerd em computação (e o fato de que em sua cela ele lê Baudrillard e Derrida, ao invés de, digamos, Schneier ou Kahn). Na trama em que um empregado do governo deve ser ludibriado a trocar a sua senha (para que um intruso possa ganhar o acesso), ao tentar dar visibilidade aos dados em rede, a obra regressa diretamente à terrível época de filmes como *A Rede* (1995), *Hackers: Piratas de Computador* (1995), *Quebra de Sigilo* (1992), *Jogos de Guerra* (1983) ou *Tron: Uma Odisseia Eletrônica* (1982). É verdade que *Hackers: Piratas de Computador* é mais lembrado por apresentar Angelina Jolie como uma das duas estudantes que se envolvem em extorsão corporativa. E também é verdade que os protagonistas passam mais tempo falando bobagens e fazendo festa do que usando computadores, mas além disso este filme exibe um vírus que fala e que tem um rosto. Já *A Rede* mostra Sandra Bullock navegando freneticamente por entre sistemas de *Bulletin Board,* como se pedir uma pizza online fosse um ato radical e subversivo. Ainda

que mostre alguns aspectos verdadeiros da rede (como os endereços de IP), o filme não faz o suficiente para fundamentá-los na realidade computacional – não era possível conectar-se a um e-mail através da *Telnet*, por exemplo. Seria necessário um endereço de *IP* e um número de porta *TCP*: o *login* de um e-mail só poderia ser iniciado após estar conectado. Também não seria possível que um vírus de um *Macintosh* de 1995 infectasse um computador mainframe.

Curiosamente, *Quebra de Sigilo* (1992), uma ficção criminal concebida durante a produção de *Jogos de Guerra* (1983), apresenta uma caixa preta capaz de quebrar qualquer tipo de criptografia computacional, ameaçando desestabilizar a economia mundial (o que já suscitava o tema da criptografia pós-quântica). Ambos os filmes tendem a se precipitar ao lidarem com a tecnologia computacional – ainda que seja possível alterar as notas de alguém no colégio a partir de um computador doméstico caso a escola seja descuidada, é impossível lançar um míssil balístico intercontinental (MBI) a partir da mesma máquina, usando apenas o mesmo modem de acesso discado. *Tron: uma Odisséia no Espaço* (1982) é marcante pelo uso pioneiro que faz da computação gráfica, mas a ideia de que se poderia entrar na rede e operá-la como se fosse a malha gráfica de um videogame teve uma influência perniciosa sobre o cinema e a televisão.

Em *A senha: Swordfish* (2001), um filme extravagante com John Travolta, encontramos uma das mais engraçadas transgressões do cinema contra a computação. No filme, o personagem de Hugh Jackman é forçado a acessar remotamente um computador do Departamento de Defesa dos Estados Unidos (supostamente através de um antigo computador mainframe *PDP10* localizado em um porão do Instituto de Tecnologia da Califórnia). Ele consegue fazê-lo batendo palmas espalhafatosamente e digitando muito rápido, enquanto é ameaçado por capangas e sexualmente coagido por uma jovem... E obviamente ele obtém o acesso em 85 segundos, mesmo tendo recém superado uma condenação que o obrigou a ficar por um longo período sem usar computadores; e é óbvio que o seu software antigo, que ficou armazenado numa fita em algum porão, ainda funciona como um *malware* destrutivo, ainda que graficamente ele pareça muito ultrapassado... Em *Superman 3* (1983), pelo menos o personagem de Richard Pryor podia se concentrar para hackear um satélite meteorológico, por mais improvável que o fosse fazê-lo utilizando uma linguagem *BASIC*, com os comandos *PRINT* e *LIST* – sem contar outras façanhas realizadas por Pryor na sua função de assistente de computação, como alterar dados de folhas salariais e desordenar semáforos.

Figura 3: Richard Pryor em *Superman 3*. Fonte: *Internet Movie Database*. Disponível em: <imdb.com/title/tt0086393>. Acesso em: 6 abr. 2020.

Figura 4: Cena de *hacking* em *A Senha: Swordfish*. Fonte: Packet Pushers. Disponível em: <packetpushers.net/a-fun-look-at-workstations-interfaces-for-it-folks>. Acesso em: 6 abr. 2020.

Infelizmente, as coisas não ficaram muito mais sofisticadas com o passar dos anos – pensemos, por exemplo, na série contemporânea *Homeland* (2011-2020): quem poderia imaginar que o servidor da CIA que os dois net-ativistas de Berlim encontram por acaso (na quinta temporada, de 2015) lhes daria acesso a um diretório repleto de arquivos, cujos longos nomes *todos* contêm a cadeia de caracteres "CIA"? Todas as listas de arquivos que você utiliza levam o nome do seu empregador? Deveríamos supor que arrancar um cabo físico da parede é a única coisa que os

peritos de Langley poderiam fazer para defender a CIA de uma enxurrada massiva de pesquisas por *cam-shows* pornô na internet? Programas como estes tendem a tratar a computação com menos seriedade do que Indiana Jones trata a arqueologia.

Isto não se trata apenas de uma questão de verossimilhança e realismo. Ainda que sabidamente o autor de ficção científica Arthur Clarke tenha declarado que qualquer tecnologia suficientemente avançada se torna indistinguível da magia, esta situação apoia-se em uma ignorância generalizada, que é legada de eras pré-letradas e é incompatível com os objetivos da educação. A magia pode ser aceita em uma ficção científica, mas não em uma universidade; nosso interesse se concentra em conceitos aplicáveis. Portanto, por exemplo, um aluno deste curso que queira discutir Harry Potter deve levar em consideração um sistema de identificação por dois fatores – para ter acesso às salas comunais de Hogwarts é necessária uma combinação de algo que você tenha (por exemplo, uma varinha) ou que você seja (não ser um "trouxa") com algo que você saiba (uma senha); sem mencionar a ofidioglossia (língua das cobras) que é necessária para acessar a câmara secreta, ou o sacrifício de sangue exigido para adentrar a caverna onde se esconde uma *Horcrux*... Como os filmes retratam o acesso restrito ao Caldeirão Furado e à plataforma 9 ¾ da estação *King's Cross*? Quem tem acesso (e como) ao banheiro dos monitores-chefes e ao escritório do professor Dumbledore? Embora estas perguntas possam soar extravagantes, são questões como estas que estão em jogo.

Antes da série *Mr. Robot* (2015-2019), raramente a televisão retratou questões de segurança da informação de maneira realista. *Mr. Robot* é sobre atividades de uma empresa de cibersegurança. Os códigos que a série mostra nas telas dos computadores são reais e não há efeitos sonoros cafonas ou arroubos de fantasia. Ao representar o hack de um aparelho celular com *Android*, pelo uso de um chip que executa um gerenciador de inicialização, a série se refere a tecnologias reais – neste caso, especificamente, ao software *Flexispy*. Notavelmente, *Mr. Robot* não se abstém de retratar os roteadores TOR, um ataque distribuído de negação de serviço (*DDoS*) em servidores corporativos e a instalação de *malwares* – neste caso, um *trojan* de acesso remoto que lembra um software verdadeiro chamado *DarkComet*.

Ironicamente, em meio à sua trama conspiratória, o pastiche sci-fi *Matrix Reloaded* (2003) é um dos poucos filmes em estilo *schlock* a mostrar uma cena realística: por uma vez ao menos evita a mania habitual de dar visualidade ao ciberespaço como se fosse um voo vertiginoso através dos desfiladeiros sombrios de uma Manhattan de dados mal renderiza-

dos. O filme mostra Trinity (nem masculina nem adolescente, mas interpretada por Carrie-Anne Moss) trabalhando com o teclado, em vez de representá-la operando alguma engenhoca qualquer com uma interface futurista. E, para encontrar vulnerabilidades na rede elétrica, ela utiliza um tipo de software existente: o NMAP, um scanner de portas TCP e UDP conhecido por gestores de sistemas no mundo todo, que é executado através de linha de comando.

Figura 5: A personagem Trinity em *Matrix: Reloaded*. Fonte: *The Killtime*. Disponível em: <thekilltime.com/the-matrix-1999>. Acesso em: 6 abr. 2020.

O *ciberthriller* alemão *Invasores: Nenhum Sistema está Salvo* (2014) apresenta de forma semelhante o uso destes softwares (*exploits*) na rede elétrica – remotamente, o protagonista Benjamin procura afetar um serviço local utilizando um *script* que parece dotado de poderes universais quando digitado em uma interface de linha de comandos. No thriller *Ultimato Bourne* (2007), a CIA hackeia o servidor de e-mail de um jornal britânico e a tela mostra um uso realista de SSH, de servidores *Postfix* com protocolos SMTP e de um servidor de nomes de domínio (DNS) em uma interface do *Unix*. No mesmo ano, outra franquia de *thrillers* apresentava um *exploit* interessante logo nos primeiros dez minutos de filme: para combater um ciberterrorista, o protagonista de *Duro de Matar 4.0* (2007) se junta a um jovem hacker. Também nos seus primeiros dez minutos, o filme sueco *Os Homens que Não Amavam as Mulheres* (2009), adaptação para as telas do livro de Stieg Larsson, mostra as habilidades computacionais de sua protagonista. Algo que o remake hollywoodiano, de 2011, não faz. No filme de super-heróis *Quarteto Fantástico* (2015, baseado nos qua-

drinhos da *Marvel*) ao menos é possível ver Sue Storm (personagem de Kate Mara) rastreando um companheiro online: sua tela pisca "*IPSCAN*", "*TRACEROUTE*" e "*PORTSCAN*" – é muito raro ver representações realistas de tecnologias de rede.

Evidentemente, enquadrar corretamente as tecnologias computacionais no audiovisual não é apenas uma questão de software e hardware; a cibersegurança também envolve engenharia social – a exploração de padrões de comportamento, oportunidades e vulnerabilidades. Ainda que os fabricantes de hardware se aproximem dos produtores de cinema e televisão para exibir os seus artefatos, tanto a indústria de software quanto o setor educacional não cansam de perder oportunidades de mostrar a computação como algo interessante, estimulante e desafiador – sem dissimulá-la. De fato, na cultura popular o *hacking* não é mais celebrado como a atividade normalmente inócua (e ocasionalmente muito lucrativa) de alguns entusiastas da computação. A televisão parou de romantizar as obsessões de nerds engenhosos e a imprensa já não fala mais tanto do "espírito virtuoso" do capitalismo digital. Ao invés disso, os jornalistas se ocupam de vender os aspectos sinistros do *hacking* como uma ameaça sistêmica e irredutível das mídias digitais. Pouco importa que até o final dos anos 1980 um hacker era apenas alguém que, sem a ajuda de manuais e através de tentativa e erro, acabava adquirindo a habilidade de operar bem os computadores. Foi só alguns anos depois que os comentadores começaram a temer que o *hacking*, quando usado maliciosamente, poderia se configurar como um problema sério e oneroso. Na maior parte do tempo, a cultura digital foi centrada no acesso, no aprendizado, na privacidade e na liberdade de expressão (Bamford, 1982; Levy, 2001; Schneier, 2004). Ainda assim, por uma mudança paradigmática na opinião pública, assim como nas políticas econômicas e em ações legais relacionadas ao ensino e às tecnologias em rede, os comentadores mais alarmistas passaram a demonizar qualquer um que tentasse acessar mais do que aquilo que a interface oficial e limitada tinha a oferecer. Tudo isso conduz ao questionamento sobre como poderiam ser elaboradas tarefas apropriadas para os alunos do curso.

Cultuar o sigilo poderia facilmente nos levar a um ressurgimento global de rumores irracionais e, infelizmente, isto é o que se vê efetivamente em boa parte da cultura da internet. O nosso futuro tende a ser consideravelmente empobrecido quando as teorias da conspiração assumem o lugar de uma cultura computacional crítica. Seguramente, ensinar os conceitos básicos de cibersegurança e algumas linhas gerais da

história da criptologia aos alunos de cinema e de estudos de mídia pode aumentar, ainda em tempo, as chances de que os seus roteiros e cenas produzam representações audiovisuais mais precisas e inteligentes da computação e da segurança da comunicação.

Para aguçar a percepção dos alunos tanto em relação às representações problemáticas da cibersegurança como quanto às possibilidades plausíveis e persuasivas de visualização da criptografia, requer-se que eles escrevam sinopses argumentativas para filmes e pilotos de TV, a partir de contos que são distribuídos entre eles. Ainda que no jargão da indústria uma sinopse seja diferente de um argumento completo (uma sinopse condensa brevemente o tom da narrativa, enquanto o argumento vai até os aspectos essenciais da representação audiovisual da estória), o que importa para os propósitos pedagógicos do curso é que este documento destaque os elementos necessários com algum ritmo e estilo cinematográfico e passe uma primeira impressão sobre as personagens, a aclimatação e os recursos visuais utilizados para evocar um tempo e um espaço. Esta sinopse argumentativa não deve apenas recontar a estória; ela deve ser suficiente para permitir que sejam tomadas decisões a partir da avaliação tanto das ideias como da solução audiovisual descrita. Além de demarcar os *beats* da narrativa com uma atenção especial à representação audiovisual dos aspectos da segurança da comunicação, o trabalho deve incluir um título e uma premissa, introduzir as personagens principais, definir os cenários, dramatizar os principais conflitos que conduzem ao clímax e esboçar uma resolução dramática. Diferente de um conto, a sinopse argumentativa não deve dizer, mas mostrar o que um personagem está pensando; não deve fornecer todo o contexto, mas esboçar alguns diálogos; por motivos pedagógicos (e porque, de fato, escrever diálogos é difícil), o objetivo neste ponto é descrever mais sucintamente alguns diálogos que o roteiro pleno iria apresentar. Os contos distribuídos entre os alunos são seleções de histórias de detetive americanas e britânicas que datam da virada do século XIX para o século XX. Ao transformarem estes materiais obsoletos em uma sinopse argumentativa, os alunos não apenas recontam uma peça de ficção. Estando particularmente atentos às formas como a comunicação secreta pode ser apresentada na tela, eles acabam atualizando e remodelando os *beats* destas narrativas aos seus próprios gostos contemporâneos.

Além disso, os alunos devem compilar materiais de referência ao modo de verbetes de enciclopédia, referindo-se a determinados nomes e conceitos importantes à história da criptologia. Esta tarefa consiste em realizar uma pesquisa (com pelo menos quatro ou cinco referências) para

definir, descrever e discutir os termos elencados ou as pessoas escolhidas, explicando claramente como cada verbete se relaciona com os tópicos do curso. Pelo menos uma das fontes de referência deve ser proveniente de um repositório online para pesquisas acadêmicas (tais como o JSTOR ou o *Project* MUSE), para que os alunos possam ir aos poucos se familiarizando aos sistemas de biblioteca que fazem parte do trabalho acadêmico. Podendo se ocupar de nomes que vão desde Alberti e Trithemius até Diffie e Schneier, e de conceitos que incluem o princípio de Kerckhoffs, as provas de conhecimento-zero, o *Atbash*, o PGP e o chip *Clipper*, eventualmente os alunos encontram dificuldades para sintetizar suas descobertas em um único verbete que seja conciso, mas ainda suficientemente abrangente. Uma avaliação em sala de aula é realizada na metade do período letivo, contendo tanto questões de múltipla escolha sobre fatos históricos como algumas questões abertas que requerem alguns parágrafos de reflexão. De que modo as palavras-chave podem ser utilizadas para aprimorar uma cifra de César? Qual é o segundo trigrama mais comum na língua inglesa? Quais tipos de tintas invisíveis você saberia citar? Qual é o nome do antigo método grego para garantir a segurança das mensagens confidenciais? Qual diplomata dos Estados Unidos está ligado aos discos cifrados? Caso não se tenha a senha, qual é o primeiro passo para começar a decodificar uma mensagem cifrada com o método de Vigenère? O que ocasionou a reviravolta estatística de Babbage na criptoanálise, e porque não foi ele, mas Kasiski quem a publicou? Como parte da avaliação, consta ainda um artigo substancial a ser escrito em casa. A escolha individual do tema e os primeiros esboços devem ser trabalhados em aula. Ao menos uma das fontes deve ser proveniente de um banco de dados online de pesquisa acadêmica, novamente, e o tema do estudo deve ser relacionado aos materiais do curso. Os governos deveriam ter a permissão para acessar a comunicação encriptada de qualquer indivíduo para prevenir crimes ou as empresas de tecnologia deveriam empregar a encriptação mais segura possível para proteger a privacidade dos usuários? Quais são as formas contemporâneas de esteganografia e quão práticas elas são na proteção e/ou transmissão de informações sigilosas através de arquivos superficialmente inalterados de áudio, de imagem, de vídeo etc.? Em todos os processos de escrita deste curso, tanto em aula como em casa, os alunos realizam avaliações por pares de diferentes esboços, através de um ambiente online compartilhado. Desta forma, ao serem avaliados, os trabalhos finais já não contêm mais as falhas e imprecisões comuns aos primeiros esboços.

Os alunos logo descobrem por conta própria o motivo pelo qual as representações audiovisuais das comunicações secretas são tão frequentemente errôneas e afetadas. Mas são poucos aqueles que conseguem encontrar soluções suficientemente criativas a ponto de serem exaltadas por seus colegas nas revisões por pares. Muitas das atividades deste curso não demandam resenhas ou comentários sobre a bibliografia, diferentemente das abordagens críticas e analíticas que geralmente são exigidas dos estudantes das Ciências Humanas. Quando a escrita objetiva contar uma história por meios audiovisuais, não basta relatar os pensamentos de uma personagem nem descrever os contextos técnicos e biográficos. Decerto, não se pode esperar uma escrita verdadeiramente criativa – os alunos sabem que não devem copiar nem inventar completamente os diálogos e as personagens de suas sinopses argumentativas. Uma vez que eles percebem como é possível manter a fidelidade à dimensão conceitual de um conto e ainda assim contribuir com ideias consideravelmente inventivas para um roteiro baseado na mesma obra, os alunos tendem a entregar-se com uma engenhosidade impressionante.

Por outro lado, mesmo que eles apreciem descobrir como escrever seus próprios nomes usando uma cifra maçônica ou que consigam expressar as diferenças entre as cifras de substituição e transposição, não se deve esperar que estudantes de Ciências Humanas instalem o *JCrypt* em seus computadores, ou que estudem a fundo a matemática envolvida na criptografia assimétrica (Koblitz, 1997; Kaur, 2008; Winkel, 2008; Kurt, 2010). Entretanto, certamente se pode confiar no seu envolvimento com uma ementa voltada a um levantamento da história da comunicação secreta que, mesmo tratando predominantemente de estágios anteriores à computação, permite que eles tirem conclusões sobre suas próprias vidas no século xxi. Mesmo (e especialmente) aqueles alunos que não forem cientistas da computação promissores devem ser capazes de debater o papel da criptografia durante a Segunda Guerra Mundial, tendo lido sobre as máquinas *Enigma* e *Purple*, sobre Alan Turing e os matemáticos poloneses que fizeram descobertas seminais naquele período. Os estudantes invariavelmente demonstram interesse na cibersegurança contemporânea, tanto em aspectos do gerenciamento de senhas quanto em questões sobre a confiança depositada nas diversas plataformas de comunicação, sejam elas *WhatsApp*, *Messenger*, *Telegram* ou *Signal*. Eles tendem a ser entusiastas das redes sociais e, em geral, muito menos céticos

em relação à mineração de dados e à publicidade digital do que sugerem as sondagens nacionais (Pew Research Center, 2017a). Eles se animam com o Telegrama Zimmermann, mas muito mais tentando imaginar o que seriam os *casus belli* equivalentes na atualidade. Eles tendem a ser bastante céticos em relação a algumas das afirmações de David Kahn sobre o porquê de os alemães terem perdido a Segunda Guerra Mundial para a inteligência norte-americana; não vilanizam nem veneram figuras como Julian Assange ou Edward Snowden, e suas discussões e trabalhos de casa mostram uma clara preferência por debater a segurança dos servidores de jogos digitais em vez da segurança das operadoras de cartão de crédito, ou a confiança nas plataformas de mídias sociais em vez das instituições políticas.

Os discentes tendem a ter discussões acaloradas e bem informadas sobre questões de identidade, anonimato e pseudônimos online. Descontentes em ficar apenas com o ponto de vista da maioria, alguns dos alunos mantêm durante todo o curso fortes reservas quanto a certos conflitos entre privacidade e segurança pública, confiança e tecnologia avançada, liberdade de expressão online e responsabilidade pessoal. Em suas sinopses argumentativas, ao atualizarem a ficção policial clássica, como o conto de Sherlock Holmes sobre os dançarinos ou um conto de Isaac Asimov sobre encriptação, os alunos demonstram criatividade, imaginando na forma do graffiti um código que permanece secreto mesmo estando visível a todos. Talvez isto não surpreenda, dado que eles possuem menos livros impressos e leem mais arquivos digitais em seus diversos dispositivos. Menos alunos se interessam por códigos escondidos em livros, tal como os que constam na segunda temporada da série *Burn Notice* (2008-2009) (uma bíblia roubada ocupa todo o enredo desta temporada), no filme *A Lenda do Tesouro Perdido* (2004) (onde as coordenadas no verso da Declaração da Independência levam ao suposto tesouro) ou no mistério *O Vale do Terror* (1915), de Sherlock Holmes, apesar da longeva popularidade do personagem na televisão e no cinema. Também não surpreende que os estudantes estejam menos interessados em códigos que envolvam mais de um idioma, mesmo que apreciem a interrelação de longa data da história da criptologia com áreas como a Tradução e a Filologia e não apenas as suas formas mais populares, como a pedra de roseta ou os processos de descodificação das mensagens alemãs e japonesas na Segunda Guerra Mundial.

Da mesma forma, os alunos tendem a mostrar uma revigorante falta de respeito pelos aspectos antiquados dos contos que se encarregam de atualizar: em vez das caixas de rapé, canetas e lenços envenenados, as suas versões destas narrativas trazem *smartphones*, boates e graffitis; em

vez de retratarem personagens escandalizadas por casos de infidelidade ou fraudes fiscais, os enredos imaginados incluem gafes em redes sociais e concursos de camisetas molhadas. Os ensaios finais entregues pelos alunos demonstram que as metas do curso foram alcançadas, pela constatação de um evidente domínio das dimensões históricas e conceituais da criptologia. É comum o recebimento de vários artigos abordando questões de falsidade ideológica e como se prevenir contra ela. Normalmente são apresentados argumentos pertinentes tanto a favor como contra o acesso do governo a *backdoors* de criptografia; alguns estudantes mais ambiciosos e com conhecimentos de informática também se dispõem a quebrar a cabeça com criptogramas ainda não resolvidos (Schmeh, 2015; Bauer 2017) ou a enfrentar o desafio de demonstrar como os princípios de Auguste Kerckhoffs (de 1883) ainda são válidos na cultura das mídias móveis de hoje.

Para introduzi-los a uma diversidade de implementações técnicas das questões estudadas no curso, os alunos também realizam breves exercícios semanais, que vão desde a instalação correta de *browsers* e redes virtuais privadas até a comparação entre gerenciadores de senhas, passando ainda pela autenticação multifator e pelos meios de fazer uma utilização segura das redes sociais. Agora que a universidade em que eles estão matriculados passou a utilizar sistemas que requerem autenticação multifator, eles estão se dando conta de que apenas o uso de senha não é suficiente para impedir o acesso não autorizado a dados individuais e institucionais; e a maioria dos alunos tende a levar a proteção de suas informações de identificação pessoal bastante a sério. Atualmente, mesmo no ambiente acadêmico as senhas são frequentemente expostas pelo uso de malwares, pelos ataques criptográficos de força bruta, *phishing* e outros *exploits*, o que torna a história e o futuro da segurança da comunicação uma fonte de novas perguntas importantes para a vida cotidiana dos alunos. Em parte, o que este curso propõe é que os estudantes descubram estes princípios básicos por conta própria, sem que o seu comportamento seja induzido, como normalmente as instituições tendem a fazer.

A integração de recursos online ao curso também ajuda a contextualizar esta situação. Uma conta no *Instagram* é um repositório de imagens da história da criptografia mais prontamente acessível do que um projetor de slides costumava ser. Além de poderem verificar diretamente pelo calendário da Fundação Museu Nacional da Criptologia[5] o que aconteceu em determinada data na história da criptologia, os alunos também podem utilizar conversores e leitores de código

5 N.T.: *National Cryptologic Museum Foundation* (ncmf). Ver: <cryptologicfoundation.org>. Acesso em: 5 abr. 2020.

morse, brincar com tipografias *Pigpen* e com geradores de anagramas. Também podem usufruir do aparato de treinamento em cibersegurança da universidade de modo muito mais informado. Me reuni por diversas vezes com os especialistas em TI do campus, responsáveis por divulgar formas seguras de agir na internet. Quer seja nas apresentações expositivas seguidas de discussão ou em mesas-redondas de regime mais concentrado, é perceptível que aqueles alunos que fizeram o curso foram melhor avaliados nos módulos de treinamento em cibersegurança da universidade do que o público geral, de acordo com enquetes relevantes (PEW RESEARCH CENTER, 2017b).

Referências

BAMFORD, James. *The puzzle palace:* inside the National Security Agency. New York: Penguin, 1982.

BAUER, Craig P. *Secret history:* the story of cryptology. Boca Raton: CRC Taylor & Francis, 2013.

BAUER, Craig P. *Unsolved!* The history and mystery of the world's greatest ciphers from Ancient Egypt to online secret societies. Princeton: Princeton University Press, 2017.

BAUER, Friedrich L. *Decrypted secrets:* methods and maxims of cryptology. Berlin: Springer, 2007.

CLEMENS, Raymond. *The Voynich Manuscript*. Yale: Yale University Pree, 2016.

DIFFIE, Whitfield; LANDAU, Susan. *Privacy on the line:* the politics of wiretapping and encryption. Cambridge: MIT Press, 2007.

GALLOWAY, Alexander. The cybernetic hypothesis. *Differences:* a journal of feminist cultural studies, n. 25, v.1, 2014, p. 107-130.

GLASS, Darren. A first-year seminar on cryptography. *Cryptologia,* n. 37, v. 4, 2013, p. 305-310.

KAHN, David. *The codebreakers*: the story of secret writing. New York: Macmillan, 1967.

KACKMAN, Michael. *Citizen spy:* television, espionage, and Cold War culture. Minneapolis: University of Minnesota Press, 2005.

KAUR, Manmohan. Cryptography as a pedagogical tool, *PRlMUS,* v. l8, n. 2, 2008, p. 198-206.

Koblitz, Neal. Cryptography as a teaching tool. *Cryptologia,* n. 21, 1997, p. 317-326.

Koblitz, Neal. Secret codes and online security: a seminar for entering students. *Cryptologia,* n. 34, 2010, p. 145-154.

Koss, Lorelei. Writing and information literacy in a cryptology first-year seminar. *Cryptologia,* n. 38, 2014, p. 223-231.

Kurt, Yesem. Deciphering an undergraduate cryptology course. *Cryptologia,* n. 34, v. 2, 2010, p. 155-162.

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

Macrakis, Kirstie. *Prisoners, lovers, and spies: the story of invisible ink from Herodotus to al Qaeda*. Yale: Yale University Press, 2014.

Schmeh, 2015. *Klaus Schmeh's List of Encrypted Books – Klausis Krypto Kolumne*. Disponível em: <scienceblogs.de/klausis-krypto-kolumne/klaus-schmehs-list-of-encrypted-books>. Acesso em: 6 abr. 2020.

Schneier, Bruce. *Secrets and lies:* digital security in a networked world. Indianapolis: Wiley, 2004.

Singh, Simon. *The code book*: the science of secrecy from Ancient Egypt to quantum cryptography. New York: Anchor Books, 1999.

Pew Research Center. *Younger Americans express more support for encryption than older adults*. 2017a. Disponível em: <pewresearch.org/internet/2017/01/26/3-attitudes-about-cybersecurity-policy/pi_01-26-cyber-03-00>. Acesso em: 6 abr. 2020

Pew Research Center. *Cybersecurity Knowledge Quiz*. 2017b. Disponível em: <pewresearch.org/internet/quiz/cybersecurity-knowledge>. Acesso em: 6 abr. 2020

Quisquater, Jean-Jacques *et al*. How to explain zero-knowledge protocols to your children. *In*: Brassard, Gilles. (ed.) Advances in cryptology. *Crypto 89,* lncs 435, 1990, p. 628-631.

Winkel, Brian. Lessons learned from a mathematical cryptology course. *Cryptologia,* n. 32, v. 1, 2008, p. 45-55.