Segurança da Informação

Márcio Moretto Ribeiro

18 de Agosto de 2017

Apresentação

Essas são notas de aula da disciplina Segurança da Informação ministrados no segundo semestre de 2017 para as turmas do período diurno e noturno do curso de Sistemas de Informação da Escola de Artes Ciências e Humanidades (EACH) da USP. A primeira versão desta apostila foi escrita para o curso de verão ministrado entre os os dias 2 e 6 de fevereiro de 2015 também no campus leste da Universidade de São Paulo. O curso de verão foi oferecido como parte das atividades do projeto de Privacidade e Vigilância do Grupo de Políticas Públicas em Acesso à Informação (GPoPAI) e foi inspirado pelo curso online oferecido gratuitamente pela plataforma Coursera e ministrado pelo professor D. Boneh.

Aos alunos que pretendem se aprofundar no tema sugerimos as seguintes referências bibliográficas:

- J. Katz e Y. Lindell - *Introduction to Modern Cryptography*
- W. Stallings - *Criptografia e Segurança da Informação*
- C. Paar e J. Pelzl - *Understanding Cryptography*

Agradecemos aos alunos que participaram do curso de verão em 2015 e dos cursos de gradução em 2016 e 2017, suas contribuião serviram de importante feedback para escrita dessas notas.

Capítulo 1

Introdução

1.1 Privacidade

As primeiras tentativas de conceitualizar a privacidade datam do final do século XIX. Em um famoso artigo de 1890, os colegas da faculdade de direito de Bosto, Louis Brandeis e Samuel Warren denunciam que o advento da fotografia instantânea e o jornalismo haviam "invadido o recinto sagrado da vida privada" ferindo o que eles apontam como o direito individual de "ser deixado em paz". Assim, eles argumentam que o escopo do direito comun (*Common Law*), que originalmente se concentrava apenas na proteção contra agreções e já havia sido ampliado para incluir a proteção à propriedade deveria ser novamente alargado para finalmente reconhecer a "natureza espiritual do homem" [WB90].

Essa visão da privacidade como proteção à intimidade ou, nas palavras dos autores, como o "direito de ser deixado em paz" é a chave de interpretação que prevalece no debate público. Duas contribuições que não fogem a esse espírito, porém, merecem destaque nessas notas introdutórias. Em um influente artigo de 1977, Richard Posner propõe que as disputas sobre direito à privacidade sejam interpretadas em sua dimensão econômica. Para Posner, as informações privadas possuem valor. De um lado há o interesse de quem busca construir uma imagem pública sobre si, uma reputação e, de outro, há o interesse de se conhecer o outro para melhor saber como se relacionar com ele ou aprender sobre sua trajetória. Caso fosse permitido qualquer tipo de intrusão à privacidade, o efeito seria um esforço maior em não revelar, ou inclusive não produzir, dados potencialmente valiosos. Assim, a questão da privacidade, se resumiria a uma questão de eficiência econômica. Caberia ao legislador regular o direito ao controle da reputação procurando um equilíbrio que maximizasse os fluxos de informação [Pos77].

O risco tanto para o indivíduo cuja paz é perturbada pelas fotos não autorizadas, quanto para aquele que perde o controle sobre sua reputação é de que algo que pertencia a sua esfera privada se tornasse pública. Para Nissenbaum, essa dicotomização entre público e privado não dá conta dos problemas associados a quebra de privacidade. Por exemplo, um paciente espera que as informações sobre sua condição de saúde sejam eventualmente compartilhadas com outros médicos ou médicas com o intuito de melhor diagnosticá-lo, assim como um cliente espera que seu gerente de banco use suas informações bancárias para sugerir-lhe melhores investimentos. Porém, há uma flagrante quebra de privacidade se as informações médicas forem compartilhadas com o banco, com quem eventualmente o paciente negociará um plano de saúde. Esse cenário exemplifica o que a autora chama de rompimento da "integridade contextual do fluxo de informações" [Nis09].

1.2 Vigilância

Associado ao tema da privacidade, mas ligado a outra matriz teórica, estão os debates sobre vigilância. Diferente dos estudos sobre privacidade cujos principais autores são juristas preocupados com o direito individual, os esttudos sobre vigilância focam em relações de poder. Foucault descreve a vigilância como uma técnica que teria alterado profundamente as formas de exercer o poder durante os séculos XVII e XIX. O poder do senhor feudal durante a idade média era exercído por meio do suplício, a pena corporal em que o açoitado pedia misericórdia eventualmente concedida. Após a revolução francesa o suplício foi sendo substituido pela prisão e aos poucos seria desenvolvida a técnica da disciplina e da vigilância. Para o autor, a imagem que melhor descreve a técnica é uma estrutura arquitetônica proposta por Jeremy Bentham no final do século XVII. Bentham arquitetou um modelo de prisão em que os vigias ficariam no centro aonde poderiam observar todas as celas, porém, aqueles que ocupam as celas não poderiam observar o vigia. A sensação constante de estar sendo vigiado introgetaria a disciplina, outra técnica deste período, nos condenados. O propósito da vigilância e da disciplina é o de produzir corpos dóceis e obedientes [Fou96].

Em 1992, em um curto texto, Giles Deleuze propos uma atualização dos conceitos de Foucault que antecipariam o que hoje compreendemos como vigilância. Na sociedade disciplinar, descrita por Foucault, durante a vida o indivíduos passa de uma instituição disciplinar a outra: da escola, ao exército, do exército à fábrica e da fábrica ao hospital. Cada instituição disciplina o indivíduo e o modela da maneira mais eficiente à instituição. Na sociedade do controle, conforme descrita por Deleuze, o poder é exercido de maneira mais intermitente e mais sutil. O indivíduo prototípico da sociedade do controle seria o endividado cujo controle atravessa as instituições [Del92].

Desde os trabalhos de Foucault, a vigilância se tornou um tema importante de investigação dentro das ciências sociais. Diversos autores escreveram trabalhos mais ou menos importantes sobre o tema. Um autor particularmente proeminente e que merece ser citado é David Lyon que escreveu uma serie de livros e organizou diversas coletâneas de artigos [Lyo94, Lyo05]. Uma entrevista de Lyon a outro importante sociólogo contemporâneo, Zigmund Bauman, produziu um livro com tradução para o português [Bau14].

1.3 Marco Regulatório

Antes ainda dos primeiros computadores, as chamadas máquinas Hollerith revolucioram a capacidade de processamento de dados. Durante a década de trinta elas dinamizaram o processamento dos dados do censo nos EUA e na década de 40 foram usadas pelos nazistas para classificar aqueles, principalmente judeus, mas também comunistas e homossexuais, que deveriam ser transportados para os guetos, dos guetos para os campos de concentração e finalmente para as câmaras de gás [Bla01]. Finda a guerra, a evolução dos modernos Estados de bem estar social Europeu e seu necessário processamento massivo de dados casou muito bem com o desenvolvimento computacional e assustou os cidadãos com sua centralidade de processamento. Assim, começaram a surgir as primeiras leis de proteção de dados pessoais.

Mayer-Schonberger argumenta que, uma vez que as leis de proteção de dados pessoais na Europa partem todas das mesmas bases e diferem apenas em detalhes, é mais frutífero estudá-las em conjunto do que seguindo uma análise comparativa. Ele propõe uma abordagem geracional como se existisse uma tendência evolutiva das normas. A primeira geração, no começo dos anos 70, focou na regulamentação técnica dessas bases centralizadas de dados. O surgimento de mini-computadores, que favorecia o processamento descentralizado, levou a uma adaptação na legislação. A segunda geração, no final dos anos 70, focou na liberdade negativa, o direito civíl de "ser deixado em paz"nas palavras de Brandeis e Warren. A autonomia do indivíduo é, porém, contraposta a sua inclusão nos programas sociais do Estado. Então, a terceira geração legislativa, em meados dos anos 80, foge um pouco das liberdades negativas e foca em uma abordagem participativa de autodeterminação informacional. A pergunta deixa de ser se alguém quer participar ou não de processos sociais, mas como. Ainda assim, porém, os indivíduos estavam em uma posição frágil nas relações de negociação o que os levava, via de regra, a abdicar dos seus direitos. A quarta geração, de meados dos ano 90, procurou de um lado equalizar as posições de negociação ainda apostando na autonomia do indivíduo, mas também incluiu diversos mecanismos mais paternalistas excluindo certas liberdades participativas e as sujeitando à proteção juridica obrigatória. Nessa fase surgem órgãos de defesa, não apenas de auxílio aos cidadãos, mas com papel decisório para delibera contra violações [MS97].

No Brasil, o Marco Civil da Internet aprovado em 2013 não aborda diretamente as questões de proteção de dados pessoais. Carecemos de um marco legal que imponha, pelo menos, que o uso de dados pessoas dependa necessariamente do consentimento explicito e informado e cuja autorização seja dada para um fim específico.

1.4 Vigilância Digital em Massa

Em 2013 Edward Snowden revelou ao mundo o alacance dos programas de vigilância em massas das agências de espionagem dos EUA. O jornalista Glen Greenwald e a cineasta Laura Poitras divulgaram o caso em uma serie de matérias e um documentário [Gre14, Poi14]. O vazamento demonstra que a agência de segurança nacional dos EUA (NSA) tem acesso a toda a comunicação por telefone e pelos principais meios de comunicação online do mundo. O moderno modelo de negócios das empresas de internet baseado na propaganda direcionada depende da construção de perfis digitais que por sua vez dependem da produção e aquisição de uma grande escala dados pessoas. Essa competição por dados pessoais cria o que chamamos de pontos únicos de falha. A violação dessas bases permitiu à NSA produzir um banco de dados pesquisável da agência possui toda comunicação pública e privada que passa pelos servidores da Google, do Facebook, da Microsof e da Apple.

A vigilância digital em massa eleva o problema da privacidade para um outro patamar. Não se trata apenas de proteger a intimidade, ou a inviolabilidade do lar, ou do controle na construção da reputação. Nesse contexto, o problema da privacidade é também coletivo. A privacidade deve ser também enchergada como um direito civil, uma limitação ao poder do estado de antecipar as ações de grupos políticos. Para tanto, é preciso de ação politica de concientização, de regulamentação para restringir o poder das empresas que controlam o armazenamento dos dados pessoais e também desnvolvimento técnico.

1.5 Segurança da Informação

A internet é um meio intrinsecamente promíscuo []. Por uma decisão de projeto, não temos controle por onde nossas informações passam quando nos comunicamos pela rede. Conforme produzimos mais informações pessoais e permitimos que elas circulem, maior o risco de quebra da integridade dos fluxos contextuais. Em particular há atores poderosos com capacidade conhecida de observar a comunicação em escala global o que traz um risco coletivo tanto à soberania nacional dos países periféricos, como o Brasil, quanto à democracia. A regulamentação, absolutamente necessaria para controlar minimamente esses processos e garantir pelo menos o consentimento no uso de nossas informações pessoais, certamente não é suficiente. A compreensão, o desenvolvimento e a difusão de ferramentas de segurança da informação, combinada com a incorporação de uma cultura de segurança [Cul01] podem colaborar nesse sentido. Concluiremos o capítulo com uma história motivadora.

Após as denúncias de Snowden houve uma espécie de consenso nos meios ativistas sobre a importância de focar forças em desenvolver ferramentas que garantissem a criptografia ponta a ponta. O paradigma mais comum de comunicação na rede é criptografar a comunicação entre cada cliente e o servidor. Como já dissemos, conforme poucos servidores consentram a maior parte da comunicaçõ online, a informação armazenada nesses servidores passa a ser um bem muito requisitado. A ideia para superar isso seria criptografar a comunicação entre clientes. Assim, a informação armazenada nos servidores não seria compreensível seja pelos engenheiros das empresa que controla a comunicação, seja para um ator externo como um hacker ou a NSA. O principal protocolo de criptografia ponta a ponta na época era o PGP, que havia sido criado no começo da década de 90, antes do advento da web. As tentativas mal sucedidas de ressucitar o protocolo logo foram substituídas por um esforço em atualizá-lo. Duas aplicações que garantiam criptografia ponta a ponta em celulares se popularizaram nesse período: Telegram e o Textsecure. A primeira foi desenvolvida por uma compania russa e oferece serviço de criptografia ponta a ponta em comunicação síncrona usando um protocolo desenvolvido por seus engenheiros. A segunda foi desenvolvida por uma pequena empresa no Vale do Silício e se inspirou no protocolo OTR, que por sua vez se inspirou no PGP, adaptando-o para o contexto assíncrono mais adequado para a comunicação móvel. Os esforços de ativistas em promover esse tipo de ferramenta culminou com a adoção do protocolo do Textsecure, rebatizado como Signal, no Whatsapp, a ferramenta de comunicação móvel mais usada no mundo todo. A popularização da criptografia ponta a ponta em grande parte da comunicação interpessoal muda muito o cenário de proteção de direitos civis e de liberdade de organização. É certo que os metadados das comunicações - quem fala com quem, quando e de onde - não estão protegidos, é certo que a maior parte da comunicação interpessoal não está livre de intrusão seja de hackers, seja de agências governamentais, é certo que há serviços - como agenda online - em que simplesmente não há alternativa segura e, portanto, é necessaria muita ação política e desenvolvimento técnico nessa área.

Capítulo 2

Cifras Clássicas

Como argumntamos no primeiro capítulo, a internet é um meio de comunicação promíscuo. As partes que se comunicam pela rede não tem controle sobre por quais caminhos sua comunicação irá trafegar. Essa característica, porém, não se restringe a esse meio. Durante o século XVIII, por exemplo, toda correspondência que passava pelo serviço de correios de Viena na Austria era encaminhada para um escritório – *black chamber* – que derretia o selo, copiava seu conteúdo, recolocava o selo e reincaminhava para o destinatário. Todo esse processo durava cerca de três horas para não atrasar a entrega. Como a Áustria, todas as potências européias desse período operavam suas *back-chambers*. As invenções do telegrafo e do rádio só facilitaram a capacidade de criar grampos, no primeiro caso, ou simplesmente captar a comunicação no segundo [Kah96].

Partiremos, portanto, do seguinte modelo de comunicação. Duas partes, o remetente e o destinatário, buscam se comunicar. Tradicionalmente denominaremos o remetente de Alice e o destinatário de Bob. Nossa suposição principal é que o canal de comunicação entre as partes é inseguro. Ou seja, assumiremos que terceiros, que denominaremos de Eva, são capazes de observar as mensagens que trafegam pelo canal de comunicação. Essa suposição é conhecida em alguns meios como "hipótese da comunicação hacker". Para efeitos deste curso, sempre assumiremos essa hipótese.

A *criptografia* (do grego "escrita secreta") é a pratica e o estudo de técnicas de comunicação segura na presença de terceiros chamados de *adversários*. Nosso primeiro desafio no curso é apresentar sistemas de comunicação que garantam a *confidencialidade*. Ou seja, toda mensagem enviada de Alice para Bob deve ser compreensível apenas para Alice e Bob e deve ser incompreensível para Eva:

$$\begin{tikzcd} & \text{Eva} \arrow[d] & \\ \text{Alice} \arrow[rr, "\text{mensagem}"] & {} & \text{Bob} \end{tikzcd}$$

Se a importância da comunicação confidencial entre civis tem se tornado cada vez mais urgente, no meio militar é difícil remontar suas origens. Suetônio (69 - 141) por volta de dois mil anos atrás descreveu como o imperador Júlio César (100 a.c. - 44 a.c.) escrevia mensagens confidenciais:

> "Se ele tinha qualquer coisa confidencial a dizer, ele escrevia cifrado, isto é, mudando a ordem das letras do alfabeto, para que nenhuma palavra pudesse ser compreendida. Se alguém deseja decifrar a mensagem e entender seu significado, deve substituir a quarta letra do alfabeto, a saber 'D', por 'A', e assim por diante com as outras."

O esquema que chamaremos de cifra de César é ilustrado pelo seguinte exemplo:

```
Mensagem: transparenciapublicaopacidadeprivada
Cifra:    XUDQVSDUHQFLDSXEOLFDRSDFLGDGHSULYDGD
```

Como descrito Suetônio, a regra para encriptar uma mensagem consiste em substituir cada letra da mensagem por aquela que está três posições a sua frente na ordem alfabética. Para descriptografar a cifra, substituir cada letra por aquela que está três posições atrás. O problema com este tipo de sistema é que basta conhecer a regra de criptografia para decifrá-lo. Em outras palavras, o segredo da cifra é sua própria regra.

Embora técnicas de criptografia e criptoanálise existam desde o império romano, foi com o advento do teléfgrafo e sua capacidade de comunicação eficiente, que o campo se estruturou. No fim do século XIX Auguste Kerckhoff estabeleceu seis princípios que as cifras militares deveriam satisfazer:

1. O sistema deve ser indecifrável, se não matematicamente, pelo menos na prática.

2. O aparato não deve requerer sigilo e não deve ser um problema se ele cair nas mãos dos inimigos.

3. Deve ser possível memorizar uma chave sem ter que anotá-la e deve ser possível modificá-la se necessário.

4. Deve ser possível aplicar a sistemas telegráficos.

5. O aparato deve ser portátil e não deve necessitar de muitas pessoas para manipulá-lo e operá-lo.

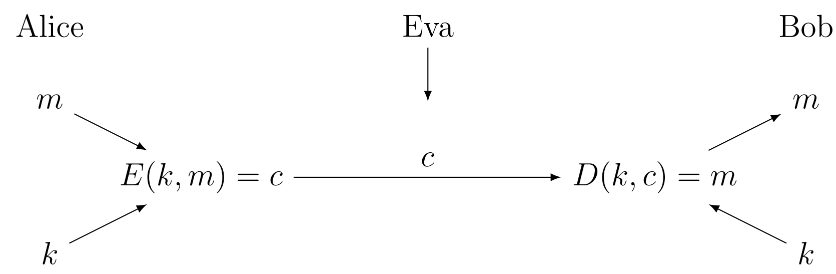
6. Por fim, dadas ascircunstâcias em que ele será usado, o sistema deve ser fácil de usar e não deve ser estressante usá-lo e não deve exigir que o usuário conheça e siga uma longa lista de regras.

O segundo princípio ficou conhecido como *princípio de Kerckhoff*. Ele estabelece que a regra usada para criptografar uma mensagem, mesmo que essa regra esteja codificada em um mecanismo, não deve ser um segredo e não deve ser um problema caso ela caia nas mãos do adversário. Nas palavras de Claude Shannon: "o inimigo conhece o sistema". Whitfield Diffie coloca o debate nos seguintes termos:

> "Um segredo que não pode ser rapidamente modificado deve ser interpretado como uma vulnerabilidade"

Ou seja, em uma comunicação confidencial as partes devem compartilhar algo que deve ser "possível de modificar caso necessário". Esse segredo compartilhado é o que chamaremos de *chave* da comunicação e assumiremos que ela é a única parte sigilosa do sistema. Trazendo o debate para uma discução mais moderna, o sigilo do código-fonte de um sistema não deve em hipótese alguma ser aquilo que garanta sua segurança.

O modelo de *criptografia simétrica*, portanto, pode ser descrito da seguite maneira: o remetente usa um algoritmo público (E) que, dada uma chave (k), transforma uma mensagem (m) em um texto incompreensível chamado de *cifra* (c), a cifra é enviada para o destinatário por um meio assumidamente inseguro (hipótese da comunicação hacker) e o destinatário utiliza a mesma chave em um algoritmo (D) que recupera a mensagem a partir da cifra.



2.1 Cifra de Deslocamento

O que chamamos na seção anterior como "cifra de César" não deve ser propriamente considerado uma cifra, pois não possui uma chave. Porém, é possível e simples adaptar esse esquema para incorporar uma chave. Para tanto faremos a seguinte alteração no esquema. Ao invés de deslocar as letras sempre três casas para frente vamos assumir que foi sorteado previamente um número k entre 0 e 23. Esse número será a chave da comunicação e, portanto, assumiremos que as partes a compartilham. O mecanismo para criptografar uma mensagem será o de deslocar cada letra k posições para a direita e para descriptografá-la basta deslocar cada letra as mesmas k posições para a esquerda.

Para formalizar este mecanismo vamos assumir que cada letra do alfabeto seja representada por um número: a letra `a` será representada pelo 0, a letra `b` pelo 1 e assim por diante. O universo de todas as chaves possíveis é o conjunto $K = \{0...23\}$ (chamaremos este conjunto de $\mathbb{Z}_{26}$ ou de maneira mais genérica $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$) e o universo de todas as mensagens possíveis é representado pelo conjunto $M = \mathbb{Z}_{26}{}^{\star}$, ou seja, todas as sequências de números entre 0 e 23. Além disso, o conjunto das possíveis cifras é $C = M$. Precisamos descrever três algorítmos:

- Gen que gera a chave $k \in K$,
- E que recebe uma chave $k \in K$ e uma mensagem $m \in M$ e produz uma cifra $c \in C$ (i.e.: $E : K \times M \rightarrow C$) e
- D que recebe uma chave $k \in K$ e uma cifra $c \in C$ e produz uma mensagem $m \in M$ (i.e.; $D : K \times C \rightarrow M$).

Um sistema de criptografia simétrica Π é formado por essa tripla de algoritmos $\Pi = \langle Gen, E, D\rangle$. Além disso, precisamos garantir que quem possui a chave seja capaz de descriptografar a cifra. Ou seja, precisamos garantir que:

$$D(k, E(k, m)) = m$$

O mecanismo que gera uma chave na cifra de substituição é bastante simples, ele simplesmente sorteia com uma distribuição de probabilidade uniforme um número entre 0 e 23. Escreveremos da seguinte forma:

$$Gen := k \leftarrow \mathbb{Z}_{26}$$

Utilizaremos a partir daqui a convenção de usar uma seta da direita para esquerda indicando que será escolhido um elemento do conjunto com probabilidade uniforme.

O algoritmo para criptografar uma mensagem traz um pequeno problema. Escreveremos $m = m_0 m_1 m_2 \ldots m_n$ uma mensagem m com $n+1$ letras cuja primeira letra é m_0, a segunda é m_1 e assim por diante. Nossa primeira tentativa de formalizar E seria somar k a cada uma das letras m_i. O problema é que esta soma pode resultar em um valor que não corresponde a nenhuma letra i.e. $m_i + k > 23$. Para evitar este problema utilizaremos não a aritmética convencional, mas a *aritmética modular*.

Dizemos que um número a divide b (escrevemos $a|b$) se existe um número inteiro n tal que $a.n = b$. Dois números são equivalentes módulo n (escrevemos $a \equiv b\ (mod\ n)$) se $n|(b-a)$. Em outras palavras, dois números são equivalentes módulo n se o resto da divisão de cada um por n for o mesmo reultado. O conjunto de todos os números equivalentes módulo n forma uma classe de equivalência que representaremos como $[a\ mod\ n] = \{b \in \mathbb{Z} : a \equiv (b\ mod\ n)\}$. Por exemplo $[5 + 7\ mod\ 10] = [2\ mod\ 10]$ pois $5 + 7 = 12$ e o resto de 12 por 10 é 2.

Estamos finalmente em condições de formalizar o sistema da cifra de deslocamento $\Pi = \langle Gen, E, D \rangle$:

- $Gen := k \leftarrow \mathbb{Z}_{26}$
- $E(k, m) = [m_0 + k\ mod\ 26] \ldots [m_n + k\ mod\ 26]$
- $D(k, c) = [c_0 - k\ mod\ 26] \ldots [c_n - k\ mod\ 26]$

Exemplo 1. *Considere a palavra* `XUXA`*. Usando a cifra de César com chave* $k = 3$ *obtemos a cifra* `BZBD`*.*

- $E(3, \texttt{24 21 24 0}) = [1\ mod\ 26][21\ mod\ 26][1\ mod\ 26][3\ mod\ 26]$

- $D(3, \texttt{1 21 1 3}) = [24\ mod\ 26][21\ mod\ 26][24\ mod\ 26][0\ mod\ 26]$

Note que $[27\ mod\ 26] = [1\ mod\ 26]$ *e que* $[-2\ mod\ 26] = [24\ mod\ 26]$.

2.2 Cifra de Substituição

Em 1567 a residência da rainha da Mary da Escócia foi destruída por uma explosão que levou a morte do então rei, primo de Mary. O principal suspeito do assinato foi dispensado da pena e se casou com Mary no mês seguinte. O episódio levou-a a prisão na Inglaterra. Neste tempo, para a maioria dos católicos, Mary era a legítima herdeira do trono inglês - ocupado pela protestante Elizabeth I. Durante o tempo na prisão Mary consiporou com aliados pela morte de Elizabeth. Em 1587 Mary foi executada pelo que ficou conhecido como a conspiração de Babington. A principal prova utilizada para a condenação foi uma troca de cartas cifradas interceptadas e decifradas [Sin04].

A cifra usada pelos conspiradores é conhecida hoje como *cifra de substituição* ou *cifra monoalfabética*. Neste tipo de criptografia, cada letra ou par de letras é substituída por um símbolo, que pode ser inclusive uma outra letra. Assim, a chave desse tipo de cifra é um alfabeto.

Exemplo 2. *Considere a seguinte chave de uma cifra monoalfabética. Neste caso os símbolos utilizados letras do mesmo alfabeto em ordem embaralhada:*

```
Alfabeto:    abcdefghijklmnopqrstuvwxyz
Permutação: ZEBRASCDFGHIJKLMNOPQTUVWXY
```

A partir desta chave podemos produzir textos substituindo cada letra pela letra correspondente na chave. Para descriptografar, basta fazer o processo inverso, a saber, substituir a letra da cifra pela do alfabeto.

```
Mensagem: transparenciapublicaopacidadeprivada
Cifra:    QOZKPMZOAKBFZMTEIFBZLMZBFRZRAMOFUZRZ
```

O desfecho da história da conspiração de Babington sugere que a cifra monoalfabética não é muito segura. De fato, no próximo capítulo discutiremos melhor as técnicas de criptonálise para este tipo de cifra. Não obstante, até o desenvolvimento das primeiras máquinas de criptografar, versões das cifras monoalfabéticas foram eram as cifras mais populares no mundo todo. Nos anos 70 a editora abril publicou no Brasil o famoso Manual do Escoteiro Mirim da Disney que apresentava uma cifra monoalfabética. Mais recentemente, o curioso caso do desaparecimento de um rapaz no Acre viralizou quando seus familiares revelaram que no seu quarto havia uma coleção de livros que ele havia escrito de maneira criptografada. Mais tarde foi descoberto que o rapaz usara uma cifra de substituição cuja chave foi eventualmente encontrada.

Para fechar esta seção buscaremos formalizar o sistema de cifra de substituição simples. Uma *permutação* sobre um conjunto Σ qualquer é uma *função bijetora* $p : \Sigma \to \Sigma$. Funções bijetoras possuem a característica de serem inversíveis, ou seja, existe $q : \Sigma \to \Sigma$ tal que $p(q(x)) = q(p(x)) = x$. A função q é chamada de *inversa* de p, é única e será representada como p^{-1}. O conjunto de todas as permutações, todas as funções bijetoras, de Σ será representado como $Perm(\Sigma)$. A chave de uma cifra de substituição é uma permutação do alfabeto $\mathbb{Z}_{26}$ escolhida aleatoriamente. Para encriptar uma mensagem basta aplicar essa permutação a cada uma das mensagens e para descriptografá-la basta aplicar a função inversa.

Formalmente temos que $\Pi = \langle Gen, E, D \rangle$ em que:

- $Gen := k \leftarrow Perm(\mathbb{Z}_{26})$
- $E(k, m) = k(m_0) \dots k(m_n)$
- $D(k, c) = k^{-1}(c_0) \dots k^{-1}(c_n)$

2.3 Cifra de Vigenère

A cifra de Vigènere foi criada no século XV e ainda no começo do século XX era considerada inquebrável – em 1868 o matemático e autor de Alice no País das Maravilhas, descreveu a cifra como "inquebrável" e um artigo da Scientific American de 1917 a descrevia como "impossível de traduzir". Veremos no próximo capítulo que há um exagero nessas descrições, porém, a sofisticação desse tipo de cifra chamado de *polialfabética* tornava sua criptoanálise muito mais sofisticado.

Em poucas palavras, a cifra de Vigenère consiste em deslocar as letras do texto original em distâncias diferentes. Em sua versão mais simples, sua chave consiste de uma palavra cuja primeira letra indica quantas casas devemos deslocar a primeira letra da mensagem, a segunda letra da chave indica quantas casa devemos deslocar a segunda letra e assim por diante. Quando a mensagem ultrapassa o tamanho da chave, repetimos a chave e continuamos o processo.

Para facilitar a conta na hora de criptografar e descriptografar, podemos usar uma tabela que indica para cada letra da mensagem e cada letra da chave qual é a letra correspondente na cifra. Essa tabela é chamada de *tabula recta* e está representada na Figura 2.1.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figura 2.1: Tabula Recta

Exemplo 3. *Considere a seguinte mensagem criptografada com a chave* `senha` *usando a cifra de Vigenère:*

`Mensagem: transparenciapublicaopacidadeprivada`

```
Chave:    senhasenhasenhasenhasenhasenhasenhas
Cifra:    LVNUSHEELNUMNWUTHVJAGTNJIVEQKPJMIHDS
```

Para fechar o capítulo vamos fazer o exercício de formalizar a cifra de Vigenère. A chave consiste em uma sequência de letras, tipicamente escolhidas em um dicionário, mas vamos aqui supor que a escolha seja aleatória e com um tamanho fixado l. A partir dessa semente, podemos gerar uma chave auxiliar k' obtida repetindo k quantas vezes forem necessárias até que $|k'| = |m| = n$. Para criptografar basta desolcar m_i por k'_i posições. Formalmente temos que $\Pi = \langle Gen, E, D \rangle$

- $Gen := k \leftarrow \mathbb{Z}_{26}^{l}$
- $E(k, m) = [m_0 + k_0{}' \ mod\ 26] \ldots [m_n + k_n{}' \ mod\ 26]$
- $D(k, c) = [c_0 - k_0{}' \ mod\ 26] \ldots [c_n - k_n{}' \ mod\ 26]$

2.4 Maquinas de Criptografar

No final da primeira década do século XX foram inventadas as primeiras máquinas de criptografar. A componente principal dessas *maquinas eletromecânicas* é um conjunto de *rotores*. A configuração inicial dos rotores contém a chave da criptografia. Cada vez que o operador pressiona uma tecla o rotor embaralha as letras. Dessa forma, essas *máquinas rotoras* se comportam como uma sofisticada cifra polialfabética. Para descriptografar a mensagem, o operador precisa ajustar a máquina em modo de descriptografia, ajustar a configuração inicial com a chave secreta e digitar o texto cifrado. A máquina então irá se rearrajar para produzir o texto original quando digitado.

As máquinas rotora mais conhecida são da série *Enigma*. Elas foram criadas por um inventor alemão no final da primeira guerra mundial e versões mais modernas foram extensamente usadas durante a segunda guerra pelo exército nazista. As versões mais simples da máquina possuiam três rotores capazes de gerar $26^3 \approx 175.000$ possíveis configurações iniciais. Além disso, era possível trocar a ordem dos rotores multiplicando por 6 o número de combinações possíveis e chegando a um total de cerca de 105 mil possibilidades. A versão utilizada pelo exercito nazista, porém, permitia cerca de 150 trilhões de possibilidades. Em 1939 Alan Turing desenvolveu uma máquina eletromecânica chamada *Bombe* capaz de decifrar algumas cifras de máquinas Enigma com 3 rotores e, posterioirmente foi melhorada para decifrar mensagens de máquinas Enigma mais sofisticadas.

A história da computação esbarra na história da criptografia neste ponto. Poucos anos antes da guerra, Alan Turing demonstrara que a satisfatibilidade da lógica de primeira ordem é um *problema indecidível*. Para tanto ele propôs um *modelo computacional* que hoje chamamos de *Máquinas de Turing*. Diferente dos modelos computacionais anteriores como o *cálculo lambda* de Church ou as *funções recursivas* de Gödel, o modelo de Turing era intuitivo. Além disso, Turing mostrou que era possível construir com seu modelo uma *Máquina Universal* capaz de simular qualquer outra Máquina de Turing. Esse resultado magnífico é o que dá origem a computação. O primeiro modelo de computador desenvolvido por Turing e sua equipe em Bechley Park foi batizado de *Colossus* e tinha como principal propósito quebrar outra cifra usada pelos nazistas durante a guerra, a *cifra de Lorenz*. A cifra de Lorenz é uma versão do que estudaremos com o nome de *cifra de fluxo*. Para decifrar os códigos das máquinas Enigma e da cifra de Lorenz os ingleses tiveram que contar, não apenas com o texto criptografado que interceptavam sem grandes dificuldades, mas também com uma série cifras cujas mensagens eles conheciam previamente. Veremos mais pra frente a importância desta informação. A capacidade dos aliados de decifrar as mensagens de seus adversários foi central para sua vitória.

O começo do século XX marcou o surgimento das primeiras máquinas de criptografar, as primeiras máquinas de criptoanálise. Na metade do século começaram a surgir os primeiros computadores. Nos anos 70 a comunicação seria revolucionada pelo advento da internet, mas antes disso já ficara claro que era necessário compreender melhor o que faz uma cifra ser segura.

2.5 Exercício

Exercício 1. *Considere a seguinte mensagem:*

```
privacidadepublicatranparenciaprivada
```

- *Criptografe essa mensagem utilizando a cifra de deslocamento com* $k = 3$.

- *Criptografe essa mensagem utilizando a cifra de substituição com a seguinte permutação de letras:* `ZEBRASCDFGHIJKLMNOPQTUVWXY`

- *Criptografe essa mensagem utilizando a cifra de Vigenère com chave* `senha`*.*

Exercício 2. *Mostre que a operação de adição + modulo n é um* anel *para qualquer valor de n. Ou seja, para qualquer $a, b, c, n \in \mathbb{Z}$ temos que:*

- associatividade*: $(a+b)+c \equiv a+(b+c)$ mod n e $(ab)c \equiv a(bc)$ mod n*

- elemento neutro*: $a+0 \equiv a$ mod n e $a.1 \equiv a$ mod n*

- inverso*: existe $-a$ tal que $a+(-a) \equiv 0$ mod n*

- distributividade*: $a(b+c) \equiv ab+ac$ mod n*

Exercício 3. *Mostre que se $n|a$ e $n|b$ então $n|(ra+sb)$ para quaisquer $r, s \in \mathbb{Z}$.*

Exercício 4. *Dizemos que a é o* inverso multiplicativo *de b em $\mathbb{Z}_n$ sse $ab \equiv 1$ mod n.*

- *Mostre que 2 é o inverso multiplicativo de 5 em $\mathbb{Z}_9$.*

- *Mostre que 6 não possui inverso multiplicativo em $\mathbb{Z}_{12}$*

Exercício 5. *Proponhe um sistema de criptografia simétrica e argumento porque ele é mais seguro do que os sistemas que vimos até aqui.*

Capítulo 3

Criptoanálise

Nos capítulos anteriores vimos uma série de cifras que a história deu conta de mostrar que não são seguras. Neste capítulo focaremos nas técnicas para quebrar essas cifras. O estudo e a análise dos sistemas de informação com a intenção de desvelar seus segredos é o que chamamos de *criptoanálise*.

3.1 Ataques Força Bruta

Uma forma universal de quebrar uma cifra é conhecido como *ataque força bruta*. Ele consiste no seguinte procedimento. O adversário utiliza o esquema D, que sempre assumimos ser de conhecimento público, numa cifra c com uma primeira tentativa de chave k_0 para produzir $D(k_0, c) = m_0$. A mensagem m_0 provavelmente não fará nenhum sentido, então o adversário repete o processo com uma outra chave k_1 e em seguida com k_2 e assim por diante até que mensagem produzida seja coerente.

Consideremos a cifra de deslocamento. Estabelecemos que uma chave nesse tipo de sistema é escolhida aleatoriamente no conjunto $\mathbb{Z}_{26}$. Assim existem exatamente 26 possibilidades de chave, porque $|\mathbb{Z}_{26}| = 26$. O número esperado de tentativas até se encontrar a chave procurada é $\frac{|K|}{2}$, neste caso 13. Ou seja, a cifra de deslocamento é muito vulnerável a ataques de força bruta porque seu universo de chaves é extremamente pequeno.

Em contraste vamos calcular o universo de chaves da cifra de substituição. Vimos que o universo das chaves de uma cifra de susbstituição é $Perm(\mathbb{Z}_{26})$. Calcular $|Perm(\mathbb{Z}_{26})|$ é um exercício simples de *análise combinatória*.

$$\begin{aligned} |Perm(\mathbb{Z}_{26}|) &= 26! \\ &= 26.25.24\ldots 1 \\ &\approx 4.10^{26} \\ &\approx 2^{88} \end{aligned}$$

O universo de chaves na cifra de deslocamento é tão pequeno que é possível testar na mão todas as possibilidades de chaves. Certamente não é possível testar as possibilidades de chaves da cifra de substituição na mão. Ataques força bruta, porém, são facilmente automatizáveis. Voltaremos a pergunta sobre o tamanho do universo de chaves para uma comunicação segura no capítulo **??**.

Exemplo 4. *Muitos dos roteadores modernos possuem um mecanismo chamado de WPS (Wi-Fi Protected Setup) que supostamente simplificaria o processo de conexão, especialmente na configuração do hardware. O WPS permite que um usuário se conecte remotamente e sem fio no roteador desde que possua um PIN (Personal Identification Number). Esse PIN é uma sequência de oito digitos de 0 a 9. Ou seja, o universo das chaves é* $10^8 \approx 2^{27}$*. Neste contexto, um ataque força-bruta é possível e toma entre 4 e 8 horas.*

3.2 Ataques de Frequência

A cifra de substituição é suficientemente segura contra ataques de força-bruta. Como vimos, porém, ela não é tão segura quanto a rainha Mary da Escócia gostaria. A forma como os funcionários da rainha Elizabeth quebraram a cifra de substituição é o que chamamos de *ataque de frequência*. A ideia por trás desse tipo de ataque é bastante simples. Na cifra de substituição, cada letra é substituída por um símbolo. Portanto, a frequência de cada símbolo em um texto suficientemente longo deve ser parecida com a frequência média de cada letra naquela língua. Por exemplo, no português, esperamos que os símbolos mais comuns sejam o `a`, o `e` e o `o`. Para piorar – ou melhorar dependendo da perspectiva – na maioria das línguas há digrafos particulares, por exemplo, no português dois símbolos repetídos provavelmente representam o `r` ou o `s` e o `h` quase sempre vem depois do `l` ou do `n`. Se o texto a ser decifrado for suficientemente longo, essas pistas podem ser suficientes para quebrar a cifra.

No seguinte trecho de “O escaravelho de ouro” de Edgar Allan Poe a personagem descreve essa técnica que ela utilizou para decifrar um texto em inglês []:

> “Ora, no inglês, a letra que ocorre com mais frequência é a letra `e`. Depois dela, a sucessão é: `a o i d h n r s t u y c f g l m w b k p q x z`. O e prevalece de tal maneira que quase nunca se vê uma frase isolada em que ele não seja predominante. Aqui nós temos, portanto, bem no início, uma base que permite mais do que um mero palpite. O uso que se pode fazer da tabela é óbvio, mas, neste criptograma em particular, não precisamos nos valer dela por inteiro. Como nosso caractere dominante é o `8`, começaremos assumindo que este é o `e` do alfabeto normal. (...)”

Em português, faz sentido separar as letras em cinco blocos, com frequência de ocorrência decrescente:

1. `a`, `e` e `o`
2. `s`, `r` e `i`
3. `n`, `d`, `m`, `u`, `t` e `c`
4. `l`, `p`, `v`, `g`, `h`, `q`, `b` e `f`
5. `z`, `j`, `x`, `k`, `w` e `y`

3.3 Ataques à “Cifra Invencível”

Apesar da fama de “inquebrável” que a cifra de Vigenère oustentou até o começo do século XX, desde a metade do século anterior já eram conhecidos métodos de criptoanálise capazes de detorratar esse tipo de cifra. Em 1854 John Hall Brock Thwaites submeteu um texto cifrado utilizando uma cifra supostamente por ele inventada. Charles Babbage, o inventor das máquinas que precederam o computador moderno, mostrou que no fundo a cifra de Thwaites era equivalente a cifra de Vigenère. Após ser desafiado, Babbage, decifrou uma mensagem criptografada por Thwaites duas vezes com chaves diferentes.

Em 1863 Friedrich Kasiski formalizou um ataque contra a cifra de Vigenère que ficou conhecido como *teste de Kasiski*. O ataque considera o fato de que a chave se repete com uma frequência fixa e, portanto, há uma probabilidade de produzir padrões reconhecíveis. Considere o exemplo extraído da Wikipédia:

Exemplo 5. `Mensagem: cryptoisshortforcryptography`
`Chave:    abcdabcdabcdabcdabcdabcdabcd`
`Cifra:    CSASTPKVSIQUTGQUCSASTPIUAQJB`

Note que o padrão CSASTP se repete na cifra. Isso ocorre porque o prefixo `crypto` foi criptografado com a mesma chave. Uma vez encontrado um padrão como este, é calculada a distância entre as repetições. Neste caso a distância é 16, o que significa que o tamanho da chave deve ser um divisor de 16 (2, 4, 8 ou 16). Com esta informação, podemos aplicar um ataque de frequência nos caracteres de 2 a 2, de 4 a 4, de 8 a 8 e de 16 a 16.

3.4 Exercícios

Exercício 6. *Calculo o tamanho do universo das chaves em uma cifra de Vigenère da forma como usada normalmente (escolhendo um palavra) e na forma como apresentamos formalmente (sequência aleatória com tamanho fixo l)?*

Exercício 7. *Construa um script que extraia um corpus do português moderno (por exemplo, textos da wikipedia) e calucule a frequência de ocorrência das letras do alfabeto.*

Exercício 8. *Em 2017 um rapaz que ficou conhecido como menino do Acre ficou dias desaparecido e deixou uma serie de livros criptografados com cifra de substituição em seu quarto. A Figura 3.1 está reproduzida uma página de um desses livros. Utilize a análise de frequência para decifrar o texto.*

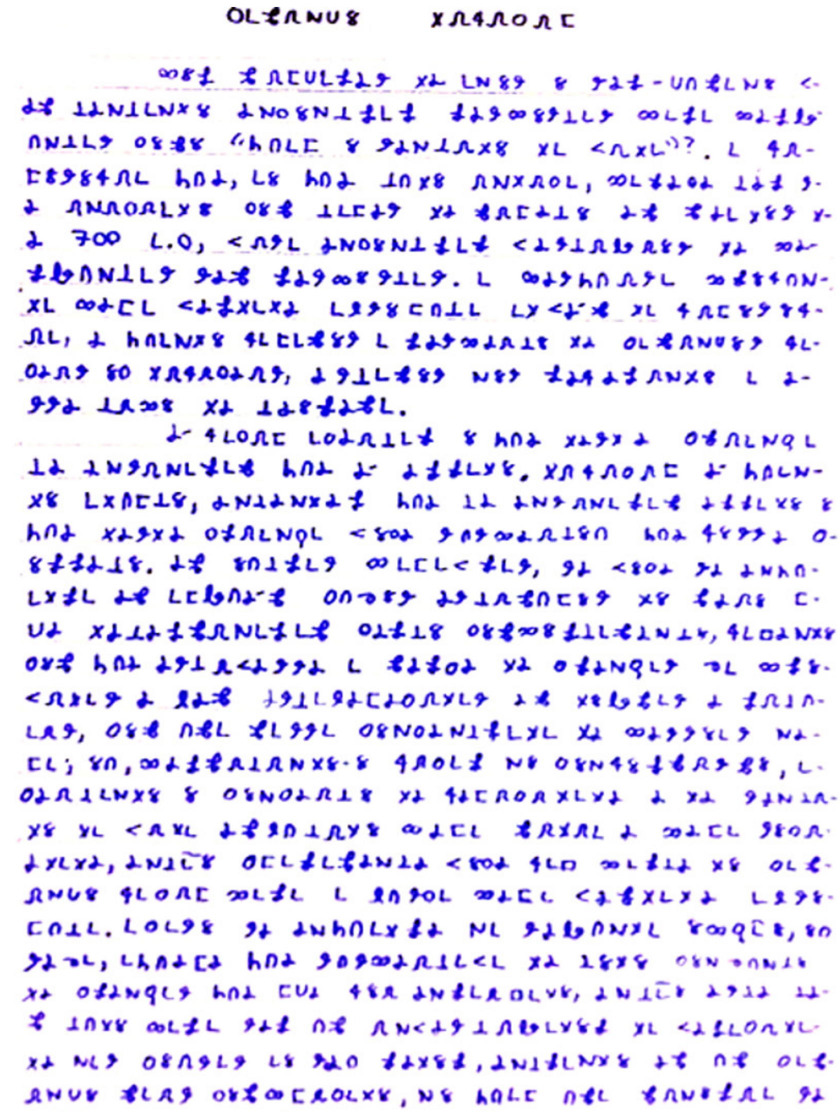


Figura 3.1: Texto criptografado pelo Menino do Acre

Capítulo 4

Sigilo Perfeito

No final dos anos 40, com o desenvolvimento dos primeiros computadores e a experiência da quebra das cifras mecanicamente produzidas por poderosas máquinas desenvolvidas pelo esforço de guerra do nazismo, alguns cientístas se voltaram para um problema central no campo da criptografia: o que torna um sistema de criptografia seguro? As cifras que vimos até agora são conhecidas como "cifras clássicas" extamente porque elas precedem desse debate moderno, e não a toa foram todas derrotadas cedo ou tarde. Informalmente, poderíamos dizer que o problema dos esquemas clássicos de criptografia é que eles guardam muita informação sobre a mensagem (frequência das letras, dos dígrafos, letras duplas etc.). Não é uma coincidência, portanto, que a primeira tentativa de formalizar o conceito de segurança tenha sido proposto por Claude Shannon, o fundador da teoria da informação. Shannon definiu o que hoje chamamos de *sigilo perfeito*. Um esquema de criptografia garante o sigilo perfeito se a cifra não guarda nenhuma informação sobre a mensagem que a gerou. Ou, de maneira um pouco mais descritiva, se a probabilidades da cifra ocorrer é independente da probabilidade da mensagem:

Definição 1. *Um esquema de criptografia simétrica* $\Pi = \langle Gen, E, D \rangle$ *garante o* sigilo perfeito *se, supondo que* $Pr[C = c] > 0$*, para toda distribuição de probabilidade sobre* M *temos que:*

$$Pr[M = m|C = c] = Pr[M = m]$$

Ou de maneira equivalente se para todo $m_0, m_1 \in M$ *e todo* $c \in C$ *temos que:*

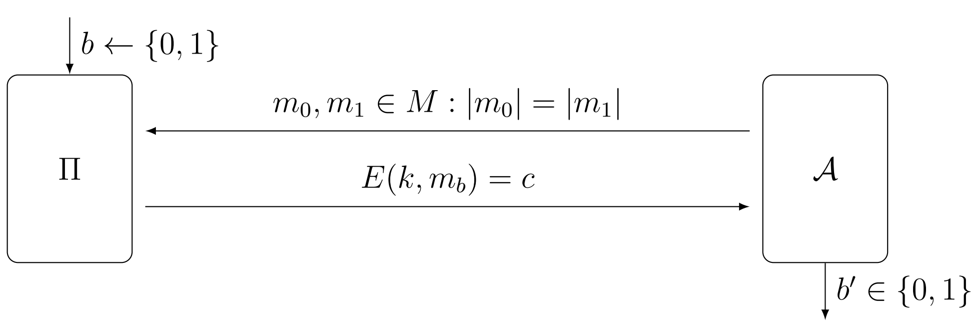
$$Pr[C = c|M = m_0] = Pr[C = c|M = m_1]$$

Essa segunda formulação é mais intuitiva, ela estabelece que um sistema garante o sigilo perfeito se a probabilidade de m_0 produzir a cifra c é idêntica a probabilidade de qualquer outra mensagem m_1 produzir a mesma cifra c. O exemplo a seguir mostra que a cifra de substituição não garante o sigilo perfeito:

Exemplo 6. *Seja* $\Pi = \langle Gen, E, D\rangle$ *o sistema de criptografia de substituição e sejam* $c = \texttt{ANA}$, $m_0 = \texttt{OVO}$ *e* $m_1 = \texttt{EVA}$. *Como o sistema* Π *substitui cada letra da mensagem por uma letra na cifra, existem chaves* k *tal que* $E(k, m_0) = c$ *– basta que* $k(\texttt{O}) = \texttt{A}$ *e* $k(\texttt{V}) = \texttt{N}$, *de fato a chance de escolher uma chave assim é* $\frac{1}{26^2} = \frac{1}{676}$ *–, mas não existe nenhuma chave* k' *tal que* $E(k', m_1) = c$. *Portanto temos que:*

$$Pr[C = c|M = m_0] = \frac{1}{676} \neq Pr[C = c|M = m_1] = 0$$

Uma forma equivalente, e útil como veremos mais para frente, de definir sigilo perfeito é a partir de um jogo. Imaginamos que há um adversário $\mathcal{A}$ cujo objetivo é quebrar a cifra produzida pelo sistema Π. O jogo funciona da seguinte maneira: $\mathcal{A}$ escolhe duas mensagens m_0 e m_1 com o mesmo tamanho ($|m_0| = |m_1|$) e envia para o sistema Π. O sistema gera uma chave k usando o algoritmo Gen e sorteia aleatoriamente uma das mensagens para criptografar (Π sorteia $b \leftarrow \{0, 1\}$ e criptografa m_b). A cifra produzida $E(k, m_b) = c$ e enviada de volta para o adversário, cujo desafia é acertar qual das duas mensagens foi cifrada. O diagrama abaixo ilustra o processo:



Chamamos o experimento ilustrado pelo diagrama de $PrivK^{eav}_{\Pi,\mathcal{A}}$. Os subscritos indicam que o experimento depende do sistema Π e do adversário $\mathcal{A}$. O resultado do experimento deve ser 0 se o adversário perdeu o desafio e 1 caso contrário. Formalmente temos que:

$$PrivK^{eav}_{\Pi,\mathcal{A}} = \begin{cases} 1 & \text{se} \quad b = b' \\ 0 & \text{c.c.} \end{cases}$$

É possível provar que um sistema Π garante o *sigilo perfeito* se e somente se para qualquer adversário $\mathcal{A}$ temos que:

$$Pr[PrivK^{eav}_{\Pi,\mathcal{A}} = 1] = \frac{1}{2}$$

Em palavras, o sistema possui sigilo perfeito se nenhum adversário é capaz de acertar qual ads mensagens produziu a cifra c com probabilidade melhor do que um meio.

4.1 One Time Pad

Temos agora uma definição formal de segurança. Vimos que a cifra de substituição não satisfaz essa definição, mas na verdade nenhuma das cifras clássica a satisfaz. Não seria desejável que essas cifras satisfizessem a definição, pois vimos no capítulo anterior que nenhuma das cifras clássicas é segura e todas podem ser derrotadas se o adversário tiver acesso a uma cifra de tamanho suficientemente grande. Ficamos então com o desafio de encontrar algum sistema que satisfaça essa definição, caso tal sistema exista.

No que segue apresentaremos um sistema chamado *One Time Pad* (OTP), também conhecida como *cifra de Vernan*, e mostraremos que ele garante o sigilo perfeito. A partir deste ponto, conforme começaremos a investigar sistemas a serem implementados computacionalmente, consideraremos que o espaço M das mensagens (assim como o espaço C das cifras) será representado como sequências de bits. No caso específico do OTP assumiremos que as mensagens e a cifras possuem um tamanho fixo n. Mais importante é o fato de que o universo das chaves é também um conjunto de sequências de bits do mesmo tamanho. Assim temos que $M = C = K = \{0,1\}^n$. O sistema $\Pi = \langle Gen, E, D\rangle$ é definido pelos seguintes algoritmos:

- $Gen := k \leftarrow \{0,1\}^n$
- $E(k,m) = [m_0 + k_0 \ mod\ 2] \dots [m_n + k_n \ mod\ 2] = m \oplus k$
- $D(k,c) = [c_0 + k_0 \ mod\ 2] \dots [c_n + k_n \ mod\ 2] = c \oplus k$

Para verificar a corretude do sistema basta notar que:

$$\begin{aligned} D(k, E(k,m)) &= D(k, k \oplus m) \\ &= k \oplus (k \oplus m) \\ &= (k \oplus k) \oplus m \\ &= m \end{aligned}$$

A derivação usa o fato de que a operação de *ou exclusivo* $\oplus$ é associativa, que $x \oplus x = 1$ e $1 \oplus x = x$ para todo sequência de bits $x \in \{0,1\}^*$. Deixamos como exercício mostrar essas três propriedades da operação.

Exemplo 7. *Considere uma mensagem* $m = 101010$ *e uma chave* $k = 010001$*. Usando o sistema One Time Pad a cifra produzida é a seguite:*

$$\begin{array}{ccccc} m & \oplus & k & = & c \\ 101010 & \oplus & 010001 & = & 111011 \end{array}$$

Como antecipado, é possível, e relativamente simples provar que o OTP possui sigilo perfeito.

Teorema 1. *O sistema de criptografia* One Time Pad *possui sigilo perfeito.*

Demonstração. Seja $K = M = C = \{0,1\}^n$. Dada uma cifra $c \in C$ e uma mensagem qualquer $m \in M$, existe uma única chave $k \in K$ tal que $E(k,m) = c$. A chave é exatamente $k = m \oplus c$, pois:

$$\begin{aligned} E(k,m) &= k \oplus m \\ &= (m \oplus c) \oplus m \\ &= (m \oplus m) \oplus c \\ &= c \end{aligned}$$

Como existe exatamente uma chave possível que faz com que $E(k,m) = c$, temos que a probabilidade se produzir c dado uma mensagem qualquer m é igual a probabilidade de sortear uma chave específica no universo $K = \{0,1\}^n$ que é $\frac{1}{2^n}$:

$$Pr[C = c | M = c] = \frac{1}{2^n}$$

Essa probabilidade é idêntica para qualquer $m \in M$. Portanto, temos que $Pr[C = c|M = m_0] = Pr[C = c|M = m_1] = \frac{1}{2^n}$. □

O *One Time Pad* possui duas severas limitações. A primeira é indicada pelo próprio nome do sistema. A sistema supõe que a chave de criptografia k seja usada exatamente uma vez ("one time"). Caso o mesmo k seja usada para criptografar duas mensagens distintas m_1 e m_2, o sistema se torna completamente inseguro.

Para ilustrar essa limitação considere que duas cifras c_0 e c_1 foram produzidas usando a mesma chave k. Assim temos que $c_0 = k \oplus m_0$ e $c_1 = k \oplus m_1$. Note o que acontece quando aplicamos o ou exclusivo entre as duas cifras eliminamos a chave:

$$\begin{aligned} c_0 \oplus c_1 &= (k \oplus m_0) \oplus (k \oplus m_1) \\ &= (k \oplus k) \oplus (m_0 \oplus m_1) \\ &= m_0 \oplus m_1 \end{aligned}$$

Uma vez eliminada a chave, é fácil separar as mensagens m_0 de m_1 utilizando um técnica similar ao ataque de frequência.

A segunda e mais crítica limitação do OTP é o tamanho de sua chave. A suposição que fizemos é que o tamanho da chave deve ser tão grande quanto a mensagem a ser cifrada. Há uma série de problemas práticos com isso. Computacionalmente não é possível gerar chaves aleatórias muito grandes, o que limita o tamanho das mensagens que podemos cifrar. Além disso, assumimos que as chaves são compartilhadas entre as partes. Deixamos os detalhes sobre a distribuição de chaves para o capítulo **??**, mas por ora podemos adiantar que se nossa chave é tão grande quanto a mensagem, porque não enviamos a mensagem pelo mesmo canal que enviaríamos a mensagem? Enfim, um sistema cuja a chave seja tão grande quanto a mensagem é de muito pouca utilidade prática.

Encerramos este capítulo mostrando que esta segunda limitação do OTP infelizmente não é uma peculiaridade do sistema. Na verdade todo sistema que possua sigilo perfeito está fadado a ter chaves tão grandes o maiores do que a mensagem. Esse resultado negativo foi proposto e demonstrado pelo próprio Shannon ainda nos anos 40.

Teorema 2 (Teorema de Shannon)**.** *Seja* $\Pi = \langle Gen, E, D \rangle$ *um sistema que garante o sigilo perfeito, então temos que* $|K| \geq |M|$.

Demonstração. Consideraremos $M(c)$ como o conjuto de todas as mensagens que podem produzir c, ou seja, as mensagens $m \in M$ tal que $E(k, m) = c$

para algum $k \in K$. É claro que $|M(c)| \leq |K|$. Agora suponha por absurdo que $|K| < |M|$. Neste caso existiria uma mensagem $m \notin M(c)$ e, portanto, $Pr[M = m] \neq 0$. Mas, por definição, temos que $Pr[C = c|M = m] = 0$ contradizendo a hipótese deu que Π garante o sigilo perfeito. $\square$

A definição de Shannon foi a primeira tentativa séria de definir segurança de sistemas de criptografia, mas o próprio autor da definição foi capaz de demonstrar suas limitações. Nos próximos capítulos apresentaremos definições de segurança mais fracas e mais úteis para nossos propósitos.

4.2 Exercício

Exercício 9. *Mostre que o* 1 *é elementro neutro na operação* $\oplus$*, ou seja, que para todo* $x \in \{0,1\}^*$ *temos que* $x \oplus 1 = 1 \oplus x = x$.

Exercício 10. *Mostre que a operação* $\oplus$ *é* associativa*, ou seja, que para todo* $x, y, z \in \{0,1\}^*$ *temos que* $x \oplus (y \oplus z) = (x \oplus y) \oplus z$.

Exercício 11. *Mostre que a operação* $\oplus$ *é* comutativa*, ou seja, que para todo* $x, y \in \{0,1\}^*$ *temos que* $x \oplus y = x \oplus y$.

Exercício 12. *Mostre que para qualquer sequência de bits* $x \in \{0,1\}^*$ *temos que* $x \oplus x = 1$.

Exercício 13. *Mostre que a cifra de deslocamento não garante sigilo perfeito.*

Bibliografia

[Bau14] Z. Bauman. *Vigilância Líquida*. Zahar, 2014.

[Bla01] E. Black. *IBM e o Holocausto: a aliança estratégica entre a Alemanha nazista e a mais poderosa empresa americana*. Editora Campus, 2001.

[Cul01] Cultura de segurança: Um manual para ativistas, 2001. Acessado em http://bit.ly/2wBcCDe em 11 de agosto de 2017.

[Del92] Gilles Deleuze. Postscript on the societies of control. *October*, 59:3–7, 1992.

[Fou96] M. Foucault. *Vigiar e punir: história da violência nas prisões*. Vozes, 1996.

[Gre14] G. Greenwald. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Henry Holt and Company, 2014.

[Kah96] D. Kahn. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, 1996.

[Lyo94] D. Lyon. *The Electronic Eye: The Rise of Surveillance Society*. University of Minnesota Press, 1994.

[Lyo05] D. Lyon. *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. Taylor & Francis, 2005.

[MS97] Viktor Mayer-Schönberger. Technology and privacy. chapter Generational Development of Data Protection in Europe, pages 219–241. MIT Press, Cambridge, MA, USA, 1997.

[Nis09] H. Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books. Stanford University Press, 2009.

[Poi14] Laura Poitras. Citizenfour. Docummentary, 2014.

[Pos77] Richard A. Posner. The right of privacy. *Sibley Lecture Series*, 22, 1977.

[Sin04] S. Singh. *O livro dos códigos*. RECORD, 2004.

[WB90] Samuel D. Warren and Louis D. Brandeis. The right to privacy. *Harward Law Review*, 4(5):193–220, December 1890.