2.
Criptografia clássica

A criptografia, ou a arte de criar códigos, constitui, assim como a criptoanálise (a arte de quebrar códigos), um ramo da criptologia, a ciência da comunicação segura. No curso da história, várias civilizações, desde as mais rudimentares, vêm desenvolvendo técnicas que permitam o compartilhamento de informação apenas entre as partes autorizadas. Atualmente, técnicas de codificação estão amplamente presentes e difundidas em nosso cotidiano, como quando se utiliza a Internet ou o cartão de crédito.

Originalmente era necessário sigilo a respeito de todo o procedimento de encriptação e decriptação de uma mensagem. Os dois principais métodos para fazê-lo consistiam na permutação dos símbolos do texto plano (mensagem original) – a transposição; e a troca dos símbolos por outros, segundo uma relação específica – a substituição. Assim, a quebra de um código criptográfico era apenas uma questão de tempo, sendo necessária a elaboração de um novo algoritmo, em um ciclo interminável.

O advento da chave criptográfica trouxe uma mudança de paradigma, permitindo que fosse possível assegurar o sigilo da comunicação com algoritmos abertos, mesmo com o envio da mensagem por um canal não-seguro. A questão da segurança passou a ser concentrada na chave, e não mais na mensagem em si. Mesmo que se saiba qual algoritmo foi utilizado para encriptar a mensagem, esta continua sendo ininteligível para qualquer um que não possua a chave. Esta deve, portanto, ser sigilosamente compartilhada pelos interlocutores, e a forma como isto ocorre classifica o tipo de criptosistema como simétrico ou assimétrico.

2.1.
Chave pública

Proposto inicialmente em 1976 (protocolo de troca de chaves Diffie-Hellman) e posteriormente implementado na forma do algoritmo RSA em 1978, o criptosistema assimétrico – ou de chave pública – opera com chaves diferentes para encriptar e decriptar a mensagem [9]. Uma das partes envia publicamente

para seu interlocutor (ou interlocutores) uma chave, com a qual este encripta a mensagem que deseja transmitir. Porém, apenas o gerador da chave possui a informação necessária para decriptar com facilidade a mensagem recebida. Tal sistema se baseia na dificuldade de se inverter determinadas funções matemáticas sem o conhecimento prévio mencionado, problema considerado muito difícil para a tecnologia computacional atual por não haver algoritmos eficientes para tal.

Neste ponto, observam-se duas falhas que levam ao questionamento da segurança deste sistema. Apesar de não haver algoritmos eficientes conhecidos para solucionar este problema matemático (basicamente fatoração de números inteiros muito grandes), não foi provada sua inexistência. Outro fato alarmante se refere ao aumento da capacidade computacional prometida para o ainda em desenvolvimento computador quântico. É previsto que, com este equipamento, poder-se-á fazer uso de um algoritmo de fatoração em tempo polinomial já desenvolvido por Shor em 1994, que reduziria drasticamente a complexidade do problema [6].

2.2. Chave privada

O outro tipo de criptosistema é conhecido como simétrico ou de chave privada. As chaves de ambas as partes comunicantes são idênticas e formadas por uma seqüência longa e aleatória de bits. Na cifra de Vernam (por ele criada em 1917 [9]), por exemplo, a chave codifica o texto plano através de uma adição módulo p. Na decriptação, a chave é novamente somada à mensagem recebida e seu conteúdo é restaurado.

A versão clássica do sistema é comprovadamente segura, desde que a chave seja utilizada uma única vez (*one-time pad*), como demonstrado por Shannon em 1949 [42]. Caso seja utilizada mais de uma vez, operações com as mensagens cifradas podem revelar parte ou a totalidade do conteúdo das mensagens.

Contudo, este sistema apresenta uma limitação fundamental. Como as chaves do transmissor e do receptor devem ser iguais, eles devem, de alguma forma, encontrarem-se pessoalmente e sigilosamente para que haja este compartilhamento. Além de dispendioso, tanto financeiramente, quanto em

relação ao tempo empregado para tal, este ato pode ser logisticamente inviável, com o agravante do requisito de uma única codificação por cada chave.