DISTRIBUIÇÃO DE CHAVES CRIPTOGRÁFICAS COM O USO DO PROTOCOLO QUÂNTICO BB84

MARIANA GODOY VAZQUEZ (FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI")
mariana.miano@fatec.sp.gov.br
GIOVANNI DELTREGGIA PANTAROTTO (FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI")
giovanni.pantarotto@fatec.sp.gov.br
RODRIGO BRITO BATTILANA (FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI")
rodrigo.battilana@fatec.sp.gov.br

RESUMO
O trabalho apresenta inicialmente o desenvolvimento da Criptografia Clássica desde os primórdios até a Criptografia Quântica, de forma breve. Discute-se a segurança dos protocolos com o advento da Computação Quântica, a Criptografia Simétrica e Assimétrica, assim como o desenvolvimento de algoritmos quânticos para diferentes tarefas. Apresenta ainda o protocolo BB84, um protocolo de distribuição de chaves criptográficas, desenvolvido juntamente com as Leis da Mecânica Quântica. O trabalho aborda, de maneira teórica, a cifra de Vernam, conhecida pelo seu alto nível de segurança, a aplicação de seu protocolo em conjunto com a cifra. Em seguida, apresenta resultados da simulação do funcionamento do protocolo BB84, desenvolvida nas condições da computação moderna, a fim de exibir e realizar testes para avaliação de desempenho, qualidade e eficiência. Por fim, tem-se as considerações sobre sua segurança, velocidade e aplicabilidade e sugerem-se estudos que possam promover melhorias no protocolo para a viabilidade de sua aplicação prática e utilização.

PALAVRAS-CHAVE: criptografia. distribuição de chaves. protocolo BB84.

A B S T R A C T
The work initially presents the development of Classical Cryptography from the beginnings to Quantum Cryptography, briefly. It discusses the security of the protocols with the advent of Quantum Computing, Symmetric and Asymmetric Cryptography, as well as the development of quantum algorithms for different tasks. It also presents the BB84 protocol, a cryptographic key distribution protocol, developed together with the Laws of Quantum Mechanics. The work approaches, theoretically, the Vernam cipher, known for its high level of security, the application of its protocol together with the cipher. Then, it presents results of the simulation of the operation of the BB84 protocol, developed under the conditions of modern computing, in order to display and carry out tests to evaluate performance, quality and efficiency. Finally, there are considerations about its safety, speed and applicability and studies that can promote improvements in the protocol for the feasibility of its practical application and use are suggested.

***Keywords**: cryptography. key distribution. protocol BB84.*

1. INTRODUÇÃO

Desde o início das civilizações, os homens se deparam com o problema de transmitir mensagens de maneira segura e intacta. Dessa necessidade, surgiu a Criptografia, ciência que estuda a comunicação secreta por meio de mensagens inteligíveis apenas aos participantes da comunicação.

Conforme apontado por Rigolin e Rieznik (2005), à medida que o mundo se moderniza, são criados mais e mais algoritmos para encriptar e decriptar mensagens, mais complexos e com menos falhas e, para esse fim, são utilizadas chaves para se manterem as mensagens secretas. Tais chaves são longas combinações de números aleatórios e manter essa chave em segredo dos que não devem participar da comunicação é o fator que define o sucesso desses protocolos. Por mais seguro que seja o canal de comunicação, nada impede que um agente externo copie a chave sem que o emissor e o receptor percebam sua presença.

Hoje, já existem protocolos que solucionam o problema de manter as chaves em segredo, o sistema de chaves públicas, de maneira que os computadores clássicos não consigam obter essas mensagens. No entanto, com a chegada da computação quântica, a segurança dos protocolos clássicos pode ser facilmente quebrada.

Visando à resolução desse problema, Marquezino (2003) cita que Bennett e Brassard (1984), criaram um protocolo que se utiliza das leis da mecânica quântica para assegurar a comunicação de forma totalmente segura, sem a possibilidade de haver a cópia dos dados da chave enviada. O protocolo, conhecido como BB84 e publicado no artigo *Quantum Cryptography: Public Key Distribution and Coin Tossing*, faz a transmissão da chave, enviando fótons que podem ser transmitidos em quatro estados de polarização diferentes, de modo que, com a aplicabilidade das leis da Mecânica quântica, garante-se a segurança do processo.

Esse trabalho tem como objetivo principal mostrar a funcionalidade do protocolo BB84, combinada ao cifrador de Vernam. De maneira geral, procurou-se demonstrar o protocolo BB84 de maneira mais simplificada, voltada para a comunicação. Como objetivo específico, pretende-se a documentação de um material teórico, a fim de fornecer material sobre o tema e análises sobre sua eficácia.

Em termos metodológicos, realizou-se inicialmente a revisão de literatura. A partir desse levantamento, construiu-se, na escrita, uma abordagem focando a implementação e demonstração do protocolo. Na análise, pretendeu-se tratar de sua funcionalidade, vantagens e desvantagens em relação à computação clássica, comparando efetividade e aplicabilidade diante dos sistemas usados atualmente, visto que o protocolo traz nova maneira de efetuar a distribuição de chaves.

2. EMBASAMENTO TEÓRICO

2.1 Surgimento e Evolução da Criptografia Quântica

De acordo com Fiarresga (2010), nos anos 90 começaram a aparecer trabalhos com computadores quânticos e algoritmos, utilizando-se da mecânica quântica. Surge, aí, a Criptografia quântica. A Criptografia quântica se mantém em alta, juntamente com os protocolos da moderna. Os processos de melhoria implementados ao longo dos anos visam a possibilidade do uso da Criptografia quântica de maneira viável e prática.

Sobral e Machado (2019, p. 204) relatam que um dos maiores impulsionadores da computação, que deu origem à computação quântica, é o aumento exponencial de processamento. Asseveram os autores que "Isso é uma das vantagens que se espera do sistema computacional baseado nos conceitos computacionais da Física Quântica: o computador quântico". A computação quântica utiliza de conceitos da física quântica, como sobreposição/superposição e entrelaçamento/emaranhamento. Não se sabe se todos os eventos da mecânica quântica são Turing-computáveis, mas alguns modelos, como as Máquinas de Turing Quânticas (MTQ), já foram construídos.

No ano de 1982, Richard Feynman apresenta um sistema quântico que poderia ser utilizado para fazer cálculos, junto com uma explicação de como tal máquina seria capaz de agir como um simulador para física quântica. Feynman também argumenta que as máquinas de Turing seriam capazes de simular fenômenos quânticos sem a introdução do fator exponencial e através disso propõe um "simulador quântico universal" (SOBRAL e MACHADO, 2019, p.211), ideia que deu origem ao computador quântico.

Grilo (2014) cita que Feynman impulsionou as pesquisas de maneiras de implementar de modo prático um computador quântico. Tais pesquisas apontavam ainda quais ganhos esses computadores poderiam trazer a partir de sua implementação.

No ano de 1994, Shor (1994) apresenta algoritmos quânticos para o problema de fatoração de números primos e para o problema do logaritmo discreto, o que propicia grande avanço, já que são pontos de grande importância em métodos criptográficos mais utilizados. Comprovou-se que, por meio da utilização de um computador quântico, eles poderiam ser facilmente quebrados.

Grover (1996), traz um algoritmo muito importante para a computação quântica, um algoritmo que faz a busca de um elemento em uma base de dados não ordenada de n elementos. Onde, com a computação clássica, seria necessário $\Omega(n)$ tempo, o algoritmo de Grover realiza a busca em $O(\sqrt{n})$, o que traz uma aceleração quadrática na solução desse problema.

Grilo (2014) afirma que, nos anos 2000, foram desenvolvidos novos algoritmos quânticos, diversos utilizando de algoritmos anteriores e apresentados vários métodos para se encontrar limitantes quânticos que resolvam diversos problemas.

2.2 Criação do protocolo BB84

Centeno (2018) descreve que em 1984 foi desenvolvido o protocolo BB84, por Charles H. Bennett e Gilles Brassard. Ambos eram cientistas que trabalhavam na área da computação quântica. Foram uns dos primeiros a trazer conceitos para a Criptografia quântica. Bennett é um físico dos Estados Unidos que desenvolveu quatro leis da informação quântica. Brassard estudou ciência da computação, mas ficou conhecido pelo seu trabalho relacionado à Criptografia quântica, teletransporte, emaranhamento e pseudo-telepatia.

O objetivo principal era criar um protocolo que executasse a distribuição de chaves entre dois usuários, com a certeza da confidencialidade da chave através de fótons polarizados enviados e recebidos por um aparelho específico, utilizando o teorema da não-clonagem e o terceiro postulado, ambos essenciais para descobrir uma ação de interferência, seja por espionagem ou cópia.

Marquezino (2003), em Estudo Introdutório do Protocolo Quântico BB84 para Troca Segura de Chaves, complementa explicando que a ideia foi buscar segurança que funcionasse de maneira a combater problemas computacionais que não possuem solução eficiente hoje, mas

ainda poderão existir. O protocolo permite que os dois usuários gerem a chave sem a necessidade de um canal secreto previamente estabelecido. O nome do protocolo se baseia nos nomes dos seus criadores Bennett e Brassard, os dois "B", e o ano em que foi criado o protocolo, 1984.

Segundo Centeno (2018), o objetivo da Criptografia é fazer com que apenas as duas partes (emissor e receptor) saibam o conteúdo da mensagem. A cifra é uma regra que informa como será executado a Criptografia, descreve passo a passo seus procedimentos e como é feita a desencriptação.

De acordo com Cavalcante (2005), a chave indica o nível de dificuldade que se tem para decodificar a mensagem. O tamanho da chave tem relação exponencial com o trabalho para decodificar, mas também com o trabalho de um agente externo de identificar qual a chave. Os tipos de chave dependem de qual tipo de Criptografia será utilizada, podendo ser uma Criptografia simétrica ou assimétrica.

A Criptografia simétrica funciona codificando um texto claro por meio de uma chave, que posteriormente será utilizada para decodificar a mensagem. Este tipo de Criptografia faz o uso de apenas uma chave que é utilizada para codificar e decodificar as mensagens. A Criptografia simétrica é geralmente usada em canais que não precisam de um grande nível de segurança, como entre computadores, internamente e externamente, ou entre máquinas.

Já na Criptografia assimétrica, são utilizadas duas chaves, sendo uma pública e a outra privada. A primeira é utilizada para cifrar a mensagem, enquanto a segunda é utilizada para decifrar a mensagem. Esse tipo de Criptografia é muito utilizado para assinatura digital e autenticação, em que a chave pública se cria a partir de uma chave privada. A chave pública pode ser enviada a todas as pessoas com quem se deseja trocar informações. Um dos algoritmos mais famosos por essa Criptografia é o RSA.

De acordo com López e Lacalle (2005), um dos grandes problemas práticos para se obter uma comunicação protegida é a troca de uma chave segura. Tal troca contribui para o sucesso dos sistemas de chaves públicas, nos quais se permite dispensar a distribuição de uma chave secreta, havendo duas chaves: a chave pública e a privada. Porém, a segurança desse método nunca foi matematicamente comprovada. Sendo possível fatorar um número inteiro em tempo polinomial, o que os computadores atuais não conseguem, haveria a quebra do nível de segurança do sistema de chaves públicas. Um computador quântico, através do algoritmo de Shor (1994), poderia desempenhar tal intento.

2.3 A Cifra associada ao protocolo BB84

Como Marquezino (2003) discute, mesmo com a melhoria trazida pelo uso do algoritmo *One-Time Pad* (utilização da mesma chave para encriptar e desencriptar, uma única vez), a dificuldade com a segurança da distribuição das chaves ainda é grande. Ele fez com que a chave chegasse ao ponto de não se repetir, porém as restrições de distribuição ainda tornavam a cifra de Vernam impraticável em muitas das aplicações, pela grande frequência da troca de chaves que a cifra demanda, bem como pela necessidade de um canal seguro, constante e rápido.

Marquezino (2003, p. 3) conclui que "Não adianta utilizar um algoritmo de chave assimétrica para trocar a chave, já que este não seria infalível, e quebrando-se este algoritmo, a Cifra de Vernam já estaria condenada."

Sobre esse assunto Tixaire (2007) complementa que "[...]a cifra de Vernam requer a utilização de chaves de "uso único" (TIXAIRE, 2007, p. 1, tradução nossa), onde cada um dos

lados necessitam dessa troca constante de chaves exclusivas, considerando que se cada chave só deve ser usada uma vez, afim de não comprometer a segurança, o protocolo BB84 traz uma possibilidade de efetuar essa troca seguindo uma boa frequência de troca já que proporciona a velocidade e segurança necessária para que se faça a troca das chaves.

Como López e Lacalle (2005) reforçam, o protocolo consegue fazer sua comunicação através de um meio público, o que permite a constância do canal. As leis da mecânica quântica garantem sua segurança, pelo Teorema da Não Clonagem.

Marquezino (2003) dá ênfase à utilização do protocolo BB84 associado à cifra de Vernam, pela sua inviolabilidade e pela alta segurança do protocolo. Cria-se, assim, uma segurança robusta. Podem-se utilizar outras cifras, porém nenhuma é, ainda, equivalente à de Vernam. A aplicação conjunta ocasiona troca de informações de maneira segura e muito competente, tornando praticamente impossível a interceptação bem sucedida das informações.

3 Desenvolvimento

3.1 Simulação da aplicação do protocolo BB84

Para a observação do comportamento do protocolo BB84, foram criados códigos de execução na linguagem Python 3.8.6, com objetivo de simulação, utilizando recursos da computação atual. Em Pantarotto (2020), buscou-se verificar como funcionaria a aplicação do protocolo. Foram criados um total de 4 códigos, dois destinados ao envio e recepção da chave polarizada, através de um canal, outros dois para que o emissor e o receptor realizem as fases do protocolo.

Para a realização da demonstração, foi utilizada uma máquina, fazendo o papel de receptor, que operou no sistema operacional Windows 7. Como emissor, utilizou-se uma máquina virtualizada, que também operou no sistema operacional Windows 7.

O protocolo foi dividido em seis fases para melhor entendimento. Durante a fase 1, o emissor faz a escolha do tamanho da entrada e insere os bits que se tornarão a chave. Para os valores de entrada, são utilizados os dígitos binários 1 e 0. O emissor insere também as bases escolhidas aleatoriamente por ele. Para a inserção da base foi utilizado “h” para a horizontal e “v” para a vertical.

Por questões de adaptação, o sistema simula a polarização através de uma operação de XOR, com a seguinte lógica: o bit 1 junto da base “v” retorna o valor 1; o bit 1 junto da base “h” retorna o valor 0; o bit 0 junto da base “v” retorna o valor 0; o bit 0 junto da base “h” retorna o valor 1. O código retorna ao emissor o resultado dessa operação de XOR (chave polarizada) para que seja enviado ao receptor.

Na fase 2, o emissor informa o valor da chave polarizada, faz a conexão entre a máquina virtual e a máquina física do autor, e executa o envio da polarização para o receptor.

Na fase 3, o receptor insere o valor da chave polarizada e faz a inserção das bases escolhidas aleatoriamente pelo receptor. Realiza-se o XOR novamente, dessa vez na chave polarizada.

Na fase 4, o receptor informa ao emissor a sequência de bases escolhidas. Na sequência, o emissor responde informando a posição em que as chaves estão divergentes entre eles. Em seguida, inserem no código a quantidade de bases divergentes e as posições delas para que sejam retiradas do valor final da chave.

Na fase 5, o receptor escolhe alguns bits para que ambos comparem os resultados, com a finalidade de detectar se houve alguma interferência externa. Então, ambos usam o código para retirá-los da chave final.

Na fase 6, a final, o emissor e o receptor recebem os valores pelo código, que são definidos como chave final, a qual será utilizada por ambos como chave da cifra.

A demonstração será exibida com uma das simulações, em que o emissor e o receptor passam pelas seis fases do protocolo BB84 enquanto se comunicam por um canal de texto diferente (chat).

Para maior aleatoriedade das informações inseridas, escolheu-se valores inseridos pelo emissor. Os valores escolhidos pelo receptor foram escolhidos por outra pessoa.

Na demonstração, durante a fase 1, o emissor define que a sequência de entrada terá 10 caracteres. Escolheu-se, como valor de entrada, a chave “1110010110” e a sequência de bases “vvhvvvhvhh”. O código devolve a sequência “1100011101”, como resultado do XOR que vai ser enviado ao receptor, conforme demonstrado na Figura 1.

Figura 1 - Emissor criando a entrada polarizada.

Fonte: Pantarotto (2020)

Feito isso, o emissor inicia a fase 2, gerando conexão com a máquina do receptor. O emissor insere a sequência “1100011101”, a mesma que chega para o receptor. Após isso, o emissor informa, pelo canal de chat, que realizou o envio. A fase 2 é ilustrada nas figuras 2, 3 e 4.

Figura 2 - Emissor enviando a entrada polarizada.

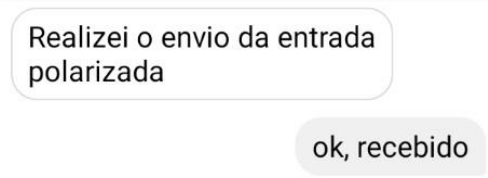
Fonte: Pantarotto (2020)

Figura 3 - Receptor recebendo a entrada polarizada.

Fonte: Pantarotto (2020)

A figura 4 ilustra a comunicação via chat entre o emissor (lado esquerdo) e o receptor (lado direito).

Figura 4 - Mensagem no chat entre ambos.



Fonte: Pantarotto (2020)

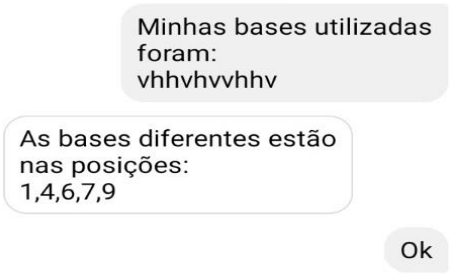
Durante a fase 3, o receptor informa a chave polarizada que recebeu do emissor, no caso "1100011101", e realiza a inserção da sequência de bases escolhidas por ele ("vhhvhvvhhv"). O receptor recebe, então, o resultado da operação XOR feita novamente (Figura 5).

Figura 1 - Receptor inserindo a entrada polarizada e as bases.

Fonte: Pantarotto (2020)

A fase 4 é aquela em que o receptor informa a sequência de bases para o emissor pelo chat. O emissor responde de volta indicando as posições que estão divergentes na escolha, conforme exposto na Figura 6, em que o emissor informa que as bases diferentes estão nas posições 1, 4, 6, 7 e 9.

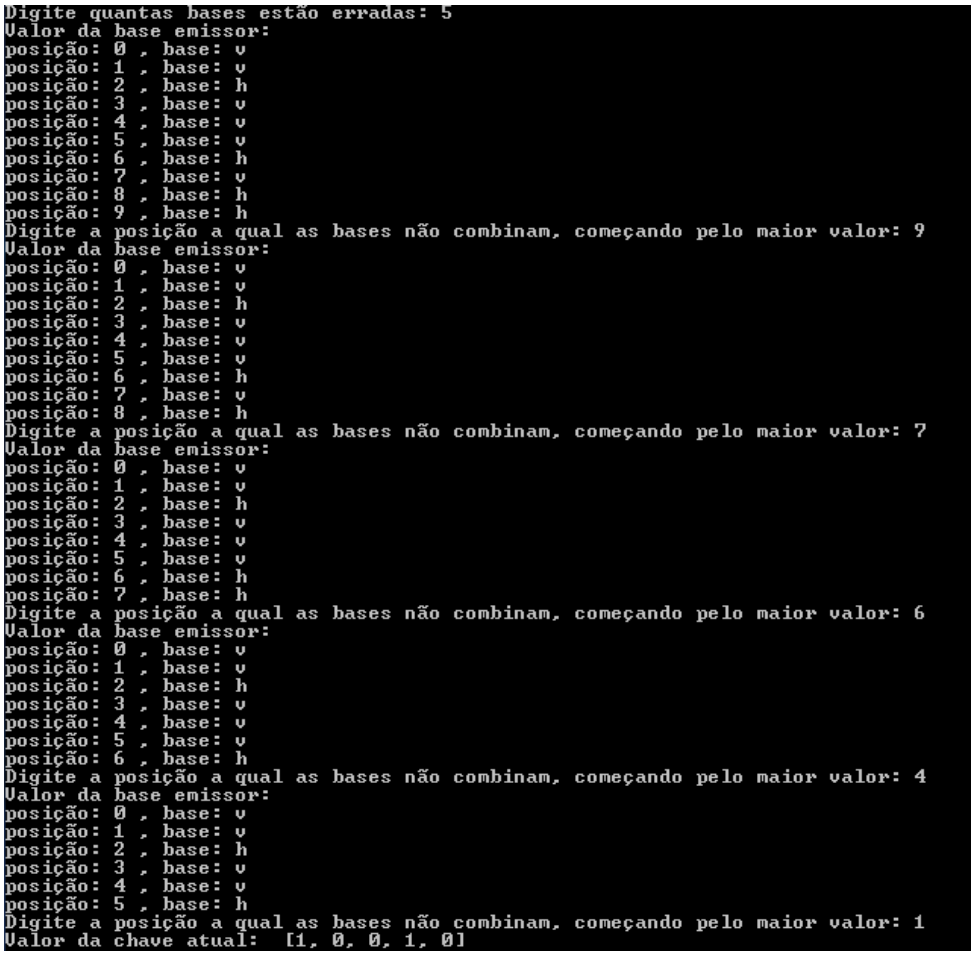
Figura 6 - Receptor envia as bases no chat e recebe as posições que estão diferentes.



Fonte: Pantarotto (2020)

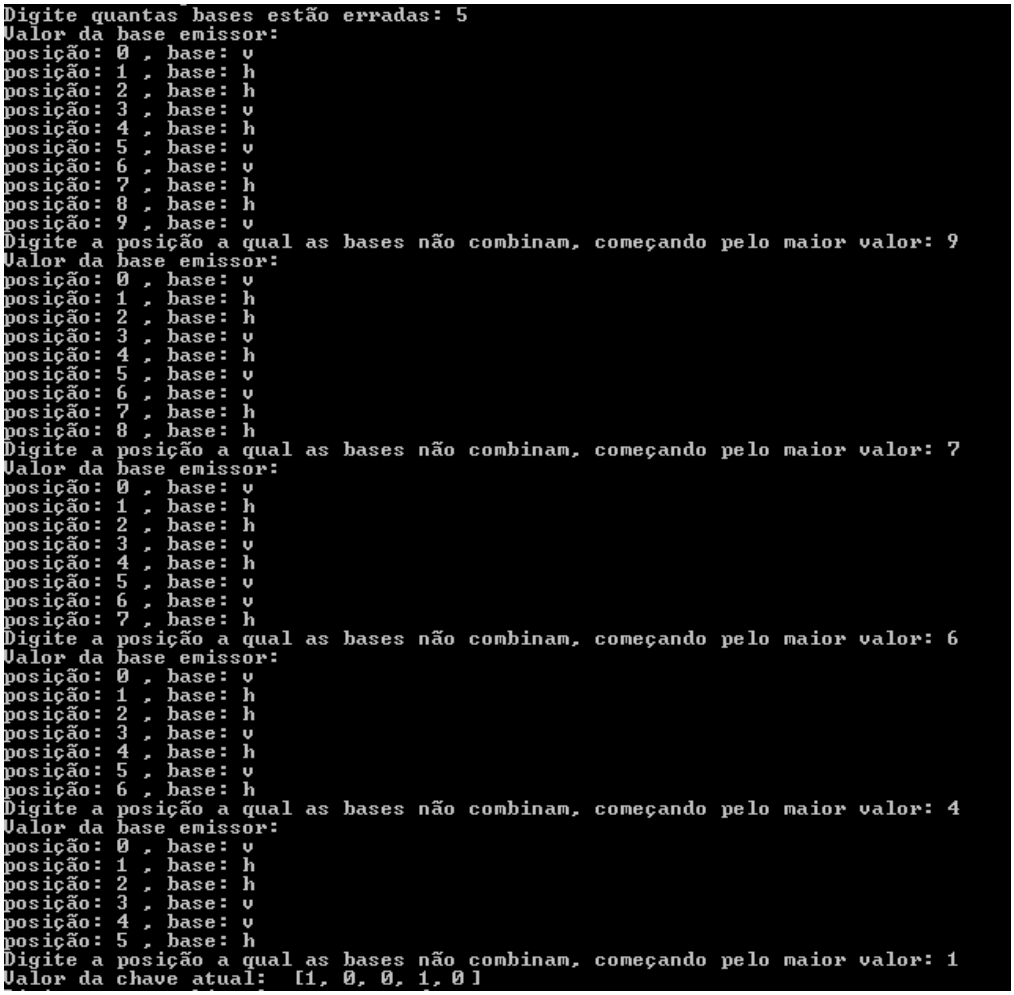
Após isso, ambos informam a quantidade e, em seguida, as bases a serem retiradas da sequência (Figuras 7 e 8).

Figura 7 - Emissor retirando as bases da sequência.



Fonte: Pantarotto (2020)

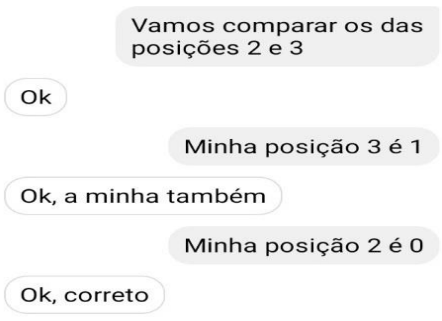
Figura 8 - Receptor retirando as bases da sequência.



Fonte: Pantarotto (2020)

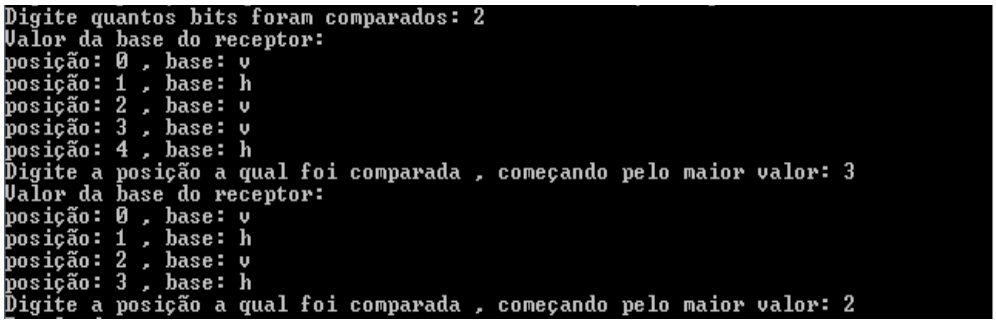
Então, se inicia a fase 5, em que o receptor escolhe alguns bits para serem comparados do valor retornado como chave atual. Na demonstração, são escolhidos dois bits (os das posições 2 e 3), considerando que as posições iniciam no zero. Os bits são comparados via chat (Figura 9) e, após isso, são informadas as posições que foram comparadas para que se retirem da chave final (Figuras 10 e 11).

Figura 9 - Comparação feita no chat.



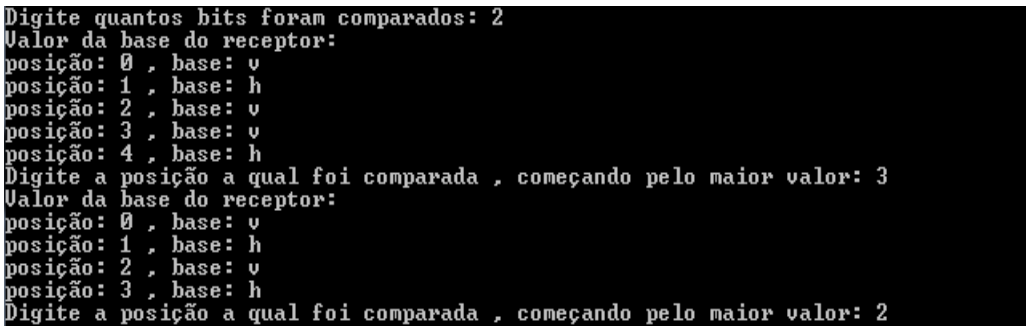
Fonte: Pantarotto (2020)

Figura 10 - Emissor retirando as posições.



Fonte: Pantarotto (2020)

Figura 11 - Receptor retirando as posições.



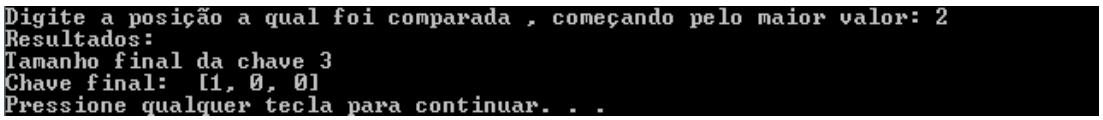
Fonte: Pantarotto (2020)

Finalizando, na Fase 6, o emissor e o receptor recebem o tamanho da chave final e sua sequência (Figuras 12 e 13). O receptor confirma via chat o tamanho da chave com o emissor (Figura 14).

Figura 12 - Emissor recebendo o tamanho e valor da chave.

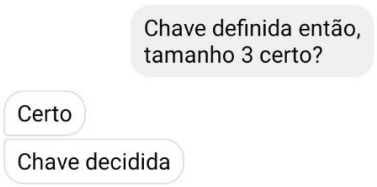
Fonte: Pantarotto (2020)

Figura 13 - Receptor recebendo o tamanho e valor da chave.



Fonte: Pantarotto (2020)

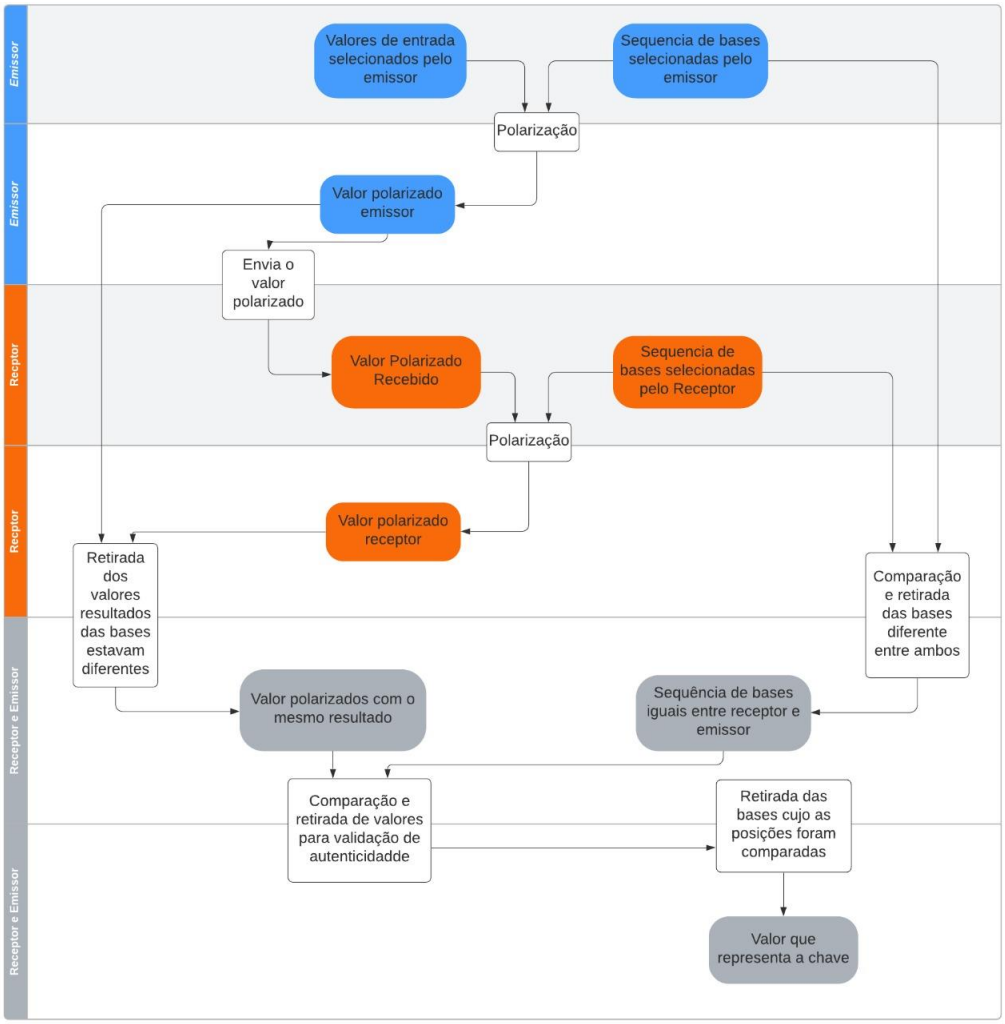
Figura 14 - Confirmação do tamanho da chave via mensagem.



Fonte: Pantarotto (2020)

Na Figura 15, é apresentado um Diagrama de Fluxo, para uma melhor compreensão e visualização da simulação do funcionamento do protocolo BB84, em suas 6 fases, até a geração da chave final (cifra).

Figura 15 – Diagrama de fluxo do funcionamento do protocolo BB84.



Fonte: Pantarotto (2020)

4 RESULTADOS E DISCUSSÃO

A partir do apresentado no decorrer do trabalho, observa-se que o protocolo BB84 traz uma grande segurança para que seja efetuada a troca de chaves criptográficas entre um emissor e um receptor. O meio de envio e a capacidade de confirmação de segurança da chave são realmente eficientes. Isso, claro, contando com a utilização de máquinas quânticas perfeitas e um canal totalmente livre de ruídos, condições necessárias para a aplicação real do protocolo. Com a aprimoração do envio e polarização de fótons, será cada vez mais possível a aplicação desse protocolo, com suas devidas e essenciais melhorias. Pode-se concluir que o protocolo traz uma segurança de alto nível computacional e, com condições físicas e lógicas ideias ainda inexistentes, otimização da velocidade de escolhas feitas pelos usuários e implementação de processos que evitem o fácil ataque por engenharia social, pode-se considerar de alta segurança para geração de chaves criptográficas.

5 CONSIDERAÇÕES FINAIS

Mesmo diante de sua eficiência, outros pontos que dificultam a aplicação são o tempo e o trabalho manual, descritos pelos autores. Considerando que a chave, por quesitos de segurança, deve ser longa e de certa complexibilidade, o protocolo faz com que o trabalho manual de seleção de chaves direcionadas a cada bit enviado seja demorado, cansativo e repetitivo. Tal circunstância tem impacto direto em sua eficiência. Em trabalhos futuros, seria interessante a proposta de melhorias em que sejam abordadas outras opções de escolha de chaves, de forma a manter a aleatoriedade, porém com maior rapidez e velocidade de processamento, por meio do desenvolvimento de um software que aprimore o protocolo BB84.

Outra questão importante a destacar é o fato de que a segurança desse protocolo se efetiva apenas de maneira computacional, contexto no qual é impossível que seja visualizado ou modificado sem deixar rastros. No entanto, ele não prevê ataques de engenharia social diretamente aplicados a um dos usuários que trocam as chaves. Em casos em que haja um atacante com nível de conhecimento computacional suficiente para fazer a captura e polarização dos dados, ele pode, na intermediação entre o emissor e o receptor, realizar trocas de fótons separadas com os dois, infiltrando-se no canal de comunicação para que ambos os usuários enviem informações a ele, mecanismo que pode permitir a manipulação das mensagens. Nesse caso, recomenda-se que um dos dois canais utilizados para a transmissão dos fótons ou das mensagens seja, de antemão, classificado como um canal seguro, a fim de vetar a apresentação do atacante como mediador entre ambos. Vale ressaltar que uma outra limitação desta técnica baseada em fótons seria seu uso em redes híbridas atuais.

REFERÊNCIAS

BENNET, C. H., BRASSARD, G. *Quantum Cryptography: Public Key Distribution and Tossing.* ***International Conference on Computers, Systems & Signal Processing.*** Vol. 1, p. 175-179, 1984.

CAVALCANTE, A. L. B. **Teoria dos Números e Criptografia.** USPIS Faculdades Integradas, 2005.

CENTENO, A. R. ***Mecánica Cuántica y comunición segura: El protocolo BB84 de Criptografía Cuántica***. 44 páginas. TCC – Universidade de Sevilla, 2018.

FIARRESGA, V. M. C. **Criptografia e Matemática.** 144 páginas. Mestrado – Universidade de Lisboa, Lisboa - Portugal, 2010.

GRILO, A. B. **Computação Quântica e Teoria da Comunicação.** 155 páginas. Mestrado – Universidade Estadual de Campinas, Campinas – Brasil, 2014.

GROVER, L. *A Fast Quantum Mechanical Algorithm for Database Search.* ***Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, STOC***, p. 212–219, New York, NY, USA, 1996. ACM.

LÓPEZ, A. G., LACALLE, J. G. L. ***Criptografía Cuántica*****.** Escola Universitária de Informática, Universidade Politécnica de Madrid, 2005.

MARQUEZINO, F. L., HEALALEY-NETO. J. A. **Estudo introdutório do Protocolo Quântico BB84 para Troca Segura de Chaves.** 15 páginas. Centro Brasileiro de Pesquisas Físicas, CCP – Coordenação de Campos e Partículas. Série Monografias, Rio de Janeiro, 2003.

PANTAROTTO, Giovanni Deltreggia. **Simulação da aplicação do protocolo quântico BB84**. 2020. Trabalho de Conclusão de Curso (Tecnologia em Segurança da Informação) – Faculdade de Tecnologia de Americana “Ministro Ralph Biasi”, Americana, 2020.

RIGOLIN, G., RIEZNIK, A. A. Introdução à Criptografia Quântica. 2005. **Revista Brasileira de Ensino de Física**, vol. 27, p. 517-526, 2005.

SHOR, P. *Algorithms for Quantum Computation: Discrete Logarithms and Factoring.* ***Proceedings 35th Annual Symposium on Foundations of Computer Science***, 35:124–134, 1994.

SOBRAL, J. B. M., MACHADO, R. B. **Computação quântica:** Aspectos Físicos e Matemáticos – Uma Abordagem Algébrica. 1ª Edição. Florianópolis: ine/CTC/UFSC, 2019.

TIXAIRE, A. G. *El Arte de Disfrazar la Información: De la C a la Q.* ***Revista E. Acad. Cienc. Exact. Fís. Nat***. Vol. 101, p. 307-320, 2007.