FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Giovanni Deltreggia Pantarotto

SIMULAÇÃO DA APLICAÇÃO DO PROTOCOLO QUÂNTICO BB84

Americana, SP

2020

FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Giovanni Deltreggia Pantarotto

SIMULAÇÃO DA APLICAÇÃO DO PROTOCOLO QUÂNTICO BB84

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Faculdade de Tecnologia de Americana "Ministro Ralph Biasi", sob orientação da professora Doutora Mariana Godoy Vazquez.

Área de concentração: Criptografia

Americana, SP

2020

Giovanni Deltreggia Pantarotto

SIMULAÇÃO DA APLICAÇÃO DO PROTOCOLO QUÂNTICO BB84

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da informação pelo CEETEPS/ Faculdade de Tecnologia de Americana “Ministro Ralph Biasi”.
Área de concentração: Criptografia.

Americana, 02 de dezembro de 2020.

Banca Examinadora:

_____
Mariana Godoy Vazquez(orientadora)
Doutora
Faculdade de Tecnologia de Americana “Ministro Ralph Biasi”

_____
Humberto Celeste Innarelli (Membro)
Doutor
Faculdade de Tecnologia de Americana “Ministro Ralph Biasi”

_____
Maria Elizete Luz Saes (Membro)
Mestre
Faculdade de Tecnologia de Americana “Ministro Ralph Biasi”

AGRADECIMENTO

Agradeço primeiramente a Deus pela saúde e força para superar as dificuldades.

À minha orientadora Prof ª Dr.ª Mariana Godoy Vazquez, ao Professor Me.° Rodrigo Brito Battilana, ao Professor Me.° Wellington Aires da Cruz Pereira e os demais professores que auxiliaram no trabalho, pela dedicação, apoio e paciência.

Ao Centro Paula Souza que me proporcionou o conhecimento necessário, a preparação, ensino e inspiração para me aprimorar e dedicar a área de segurança e buscar melhorar meus conhecimentos.

Aos que de alguma forma deram suas contribuições a realização dos estudos, pesquisas e aplicações que foram necessárias, sendo de forma direta e indireta.

Por fim, agradeço aos meus familiares e amigos, pela contribuição com o apoio, auxílio, paciência, incentivo e compreensão durante todo o desenvolvimento do trabalho.

RESUMO

O presente trabalho constitui-se de uma apresentação da Criptografia desde os tempos antigos até o desenvolvimento da computação moderna, abordando, brevemente, a computação quântica. Procurou-se explicar os conceitos básicos do funcionamento das criptografias simétricas e assimétricas e o conceito de chave para a Criptografia, abordando, assim, algumas das cifras já existentes, que são métodos de reescrever caracteres em forma de algarismos e números. Conceitua-se o protocolo BB84, um protocolo de distribuição de chaves criptográficas, explicando sua criação, funcionamento e fatores de segurança, bem como suas vantagens e desvantagens. O trabalho explora, ainda, os diversos ataques já conhecidos e perpetrados no mundo todo, tanto de maneira computacional quanto voltado à engenharia social. 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 uma simulação do funcionamento do protocolo BB84, nas condições da computação moderna, programada e simulada pelo autor, a fim de exibir e realizar testes para avaliação de desempenho, qualidade e eficiência. Por fim, apresentam-se 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; Segurança; Simulação; Protocolo BB84.

ABSTRACT

The present work consists of a presentation of cryptography from ancient times to the development of modern computing, covering, briefly, quantum computing. We tried to explain the basic concepts of symmetric and asymmetric cryptography and the key concept for cryptography, thus addressing some of the existing ciphers, which are methods of rewriting characters in the form of algorithms and numbers. The evolution of cryptography through the ages was discussed, and then the BB84 protocol, a protocol for distributing cryptographic keys, is explained, explaining its creation, operation, and security factors, as well as its advantages and disadvantages. Also brought are the various attacks already known and perpetrated around the world, both in a computational way and aimed at social engineering. The work theoretically addresses the Vernam cipher, known for its high level of security, the application of its protocol in conjunction with the cipher. Then, presents practical simulation of the BB84 protocol operation, under the conditions of modern computing, programmed and simulated by the author, in order to display and perform tests to evaluate performance, quality and efficiency. Finally, considerations about its safety, speed and applicability are presented and studies are suggested that can promote improvements in the protocol for the feasibility of its practical application and use

***Keywords**: Cryptography; Security; Simulation; Protocol BB84;*

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

MQ – Mecânica Quântica.

MTQ - Máquinas de Turing Quânticas

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 Charles Bennett e Gilles Brassard, em 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, optou-se por realizar uma revisão de literatura, por meio da leitura de artigos de artigos, monografia, teses, projetos, testes e livros. A partir desse levantamento, construir, 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.

O trabalho foi estruturado em 7 capítulos. O primeiro introduz todo o trabalho de maneira resumida, o segundo traz a história do surgimento da Criptografia e sua evolução até os dias de hoje, com a computação quântica. O terceiro capítulo traz uma explicação do funcionamento de cifras criptográficas simétricas e assimétricas; o quarto capítulo discute o funcionamento do protocolo BB84, sua implementação e falhas que podem ser encontradas. No quinto capítulo, discorre-se brevemente sobre sua eficiência junto da Cifra de Vernam; no sexto, abordam-se alguns testes de implementação e simulação do algoritmo pelo autor, de forma simplificada. Finalmente, o sétimo é construído com base nas informações dos capítulos anteriores e traz as considerações do autor sobre sua aplicabilidade e sugestão de possíveis estudos para melhorias de segurança.

2 HISTÓRIA DA CRIPTOGRAFIA – DOS PRIMÓRDIOS À COMPUTAÇÃO QUÂNTICA

Conforme citado por Ikram e Mohsen (2018, p. 1, tradução nossa) “A necessidade de garantir maneiras de se comunicar, vem desde as mais antigas civilizações, [...]” [1]. As antigas civilizações já buscavam desenvolver recursos mais eficazes para que pudessem preservar seu território e seu poder. Nesse contexto, a comunicação necessitava de um nível de segurança que possibilitasse que, através de um código implementado, suas mensagens fossem ocultadas aos que não tinham o conhecimento do código.

De acordo com Fiarresga (2010), um dos primeiros modelos datados foi encontrado no Egito, onde eram usados hieróglifos que não eram semelhantes ou compreendidos pelo resto da população. O objetivo era modificar as mensagens a fim de que apenas alguns determinados egípcios pudessem entendê-las. Esse é considerado, até os dias atuais, como o registro criptográfico mais antigo. Entretanto, como citado por Kahn (1973), a Criptografia surgiu de várias maneiras e em vários locais. Ainda que com suas peculiaridades, cada um dos modelos visava ao mesmo objetivo, ou seja, esconder o significado de mensagens.

Fiarresga (2010) ainda cita alguns métodos da Palestina, os mais antigos já compreendidos, que os Hebreus utilizavam para ocultar informações. Esses métodos dividiam-se em três grandes tipos: a cifra de Atbash, Albam e Atbah. Todas eram cifras de substituição, uma vez que as letras do alfabeto eram substituídas por outras em uma devida ordem, demandando a reescrita da mensagem que seria enviada.

Uma das cifras que ficou mais popular foi a chamada cifra de César. Embora de baixa complexibilidade, foi de extrema eficiência durante o império romano, na época de Julio César, aproximadamente 60 a.C. A cifra de César é uma cifra de substituição em que as letras do alfabeto cifradas são resultado do avanço da ordem das letras do alfabeto em três posições para a direita, conforme mostrado no quadro 1.

1 “The need to secure communication is eternal. Since the earliest civilization [...]“

Quadro 1– Operação da Cifra de Cesar.

letra → letra correspondente
A → D
B → E
C → F
D → G
E → H
F → I
e assim por diante

Fonte: Barbosa e Cornelissen (2017, p. 154).

Fiarresga (2010) acrescenta que em vários lugares foram surgindo novas técnicas que funcionavam de diferentes formas e maneiras de uso. Quanto mais o mundo evoluía, maior era a necessidade de gerar novas cifras, já que as utilizadas acabavam se tornando obsoletas e fáceis de se identificar.

No decorrer dos anos, a Criptografia foi se modificando e evoluindo. Tornou-se algo feito de maneira eletrônica, através de máquinas com alta capacidade de processamento. Com a evolução da Criptografia, surgiu também em 1855 a criptoanálise, que consiste em estudar maneiras de decifrar mensagens criptografadas. Na época, as cifras ainda eram monoalfabéticas. Assim a criptoanálise desenvolveu um método por meio do qual, em poucas mensagens, era possível realizar grande avanço na leitura da mensagem original, com base na análise de frequência da utilização das letras, como demonstra o quadro 2.

Durante a história podem-se citar grandes influências da Criptografia e suas cifras: a cifra ADFGVX usada pelos alemães no final da Primeira Guerra Mundial; a cifra da máquina Enigma usada pelos alemães na Segunda Guerra Mundial; a cifra ASCII (American Standard Code For Information Interchange), uma das primeiras cifras a utilizar números binários; a cifra DES (Dat Encryption Standard); a cifra assimétrica RSA (Rivest Shamir e Adleman), que trouxe a chave assimétrica, entre várias outras.

Quadro 2 – Frequência relativa de cada uma das letras, na língua Portuguesa.

Letra	%	Letra	%	Letra	%	Letra	%
A	12,71%	H	0,74%	O	11,32%	V	1,36%
B	0,81%	I	7,18%	P	3,07%	W	0,02%
C	4,16%	J	0,21%	Q	1,41%	X	0,28%
D	5,52%	K	0,00%	R	6,47%	Y	0,02%
E	11,99%	L	3,23%	S	7,99%	Z	0,37%
F	1,34%	M	4,48%	T	5,31%		
G	1,32%	N	5,24%	U	3,44%		

Fonte: Fiarresga (2010, p. 10).

Como Ikram e Mohsen (2018) descrevem, citando Kerckhoffs, que em 1883 publicou seu artigo “Modern Cryptography”, as primeiras civilizações não usavam realmente códigos e sim técnicas para esconder a existência de uma mensagem. Esse período é denominado Criptografia antiga. Kerckhoffs menciona o começo de um novo meio de classificação criptográfica: a Criptografia moderna. A segurança de um sistema de Criptografia moderna deve ser direcionada para a chave e todos seus outros parâmetros que possam ser conhecidos publicamente. Ikram e Mohsen (2018) confirmam essa afirmação, com o artigo de doutorado de Shannon, “The maxim of Shannon”, no qual ele demonstra que a segurança do protocolo criptográfico depende do tamanho da chave, cuja segurança deve durar, no mínimo, até que a mensagem seja codificada. Nesse sentido, deve-se garantir a segurança da mensagem pelo fato de cada chave ser utilizada apenas uma vez, assim o tempo para um interceptador decifrar a mensagem é maior que a validade de seu valor. Esse processo baseia-se nos critérios dos protocolos *one-time-pad*[2].

De acordo com o descrito por Fiarresga (2010), nos anos 90 começaram a aparecer trabalhos com computadores quânticos e algoritmos, utilizando-se da mecânica quântica. Surge, aí, a Criptografia quântica, tema que será abordado no próximo capítulo. 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.

[2] Protocolo que surgiu de uma melhoria na cifra de Vernam. Propõe uma chave que seja tão grande quanto a mensagem e não possa ser repetida. (STALLINGS, 2015)

2.1. BREVE HISTÓRIA DA COMPUTAÇÃO QUÂNTICA

Como Sobral e Machado (2019, p. 204) relatam, 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.

As máquinas clássicas são “computacionalmente equivalentes” sob determinadas rotulações dos seus estados de entrada e saída, porém não há razões lógicas para que se construam máquinas infinitamente mais poderosas. Já que a lógica não proíbe o cálculo físico de funções arbitrárias, a física o faz. Como já conhecido, ao fazer máquinas de computação, a máquina atinge rapidamente um ponto em que hardwares não alteram o conjunto de funções computáveis pela máquina. Todas as funções dentro desse conjunto sempre estarão contidas em um outro conjunto que pode ser calculado pela máquina de computação universal Turing como descrito em 1936 em *On the Computable Numbers with an application to the Entscheindugproblem.*

No mesmo ano Turing e Church criam a hipótese de Church-Turing, como citado no parágrafo:

> Church e Turing (1936) conjecturaram que essas limitações sobre o que pode ser computado não são impostas pelo estado-da-arte na concepção de máquinas de computação, nem pela nossa ingenuidade em construir modelos para computação, mas são universais. Isso é chamado de "Hipótese de Church-Turing"; de acordo com Turing:
> *Every ’function which would naturally be regarded as computable’ can be computed by the universal Turing machine.* (1)
> "Toda função naturalmente considerada como computável, pode ser computada pela máquina universal de Turing (SOBRAL; MACHADO, 2019, p. 206).

Sobral e Machado (2019), citam que, em 1982, Benioff construiu um modelo dentro da cinemática e da dinâmica quântica, mas que ainda foi classificado como um

modelo clássico, uma vez que, da maneira como foi construído, nenhuma propriedade de característica quântica era detectada no final de cada etapa computacional.

No mesmo ano, Richard Feynman traz 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.

Deutsch (1989) apresenta dois modelos computacionais quânticos, as máquinas de Turing Quânticas e os Circuitos Quânticos, os quais permitiram desenvolvimentos de algoritmos quânticos compatíveis com os futuros computadores quânticos.

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 Ω(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.

Completa Grilo (2014) que, mais recentemente, os estudos na área têm se voltado ao desenvolvimento de argumentos quânticos em teoremas puramente clássicos e meios de generalizar as técnicas já existentes a fim de criar um *framework*

para que seja realizada a aplicação a outros problemas através de um método probabilístico.

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.

3 INTRODUÇÃO À CRIPTOGRAFIA

Como mencionado por Bianchetti *et al.* (2012), a palavra Criptografia se origina do grego “Cryptos”, que significa secreto ou oculto. Criptografia é uma ciência que estuda princípios e técnicas para que sejam escritas mensagens em códigos, de maneira que apenas o destinatário consiga ler a mensagem claramente e que, para qualquer outra pessoa, o texto seja incompreensível.

Antes de explicar e exemplificar a Criptografia, alguns esclarecimentos sobre a Criptografia, nas palavras de Rezende (2019).

> A garantia de 100% de segurança é uma falácia, mas podemos trabalhar em direção a 100% de aceitação de riscos. Fraudes existem nas formas usuais de comércio: dinheiro pode ser falsificado, cheques adulterados ou roubados, números de cartão de crédito copiados. Mesmo assim esses sistemas ainda têm sucesso porque seus benefícios e conveniências compensam as perdas. Cofres, fechaduras e cortinas – mecanismos de privacidade – não são perfeitos mas, com frequência são bons o suficiente. Um bom sistema criptográfico atinge o equilíbrio entre o que é possível e o que é aceitável (REZENDE, 2019, p. 5).

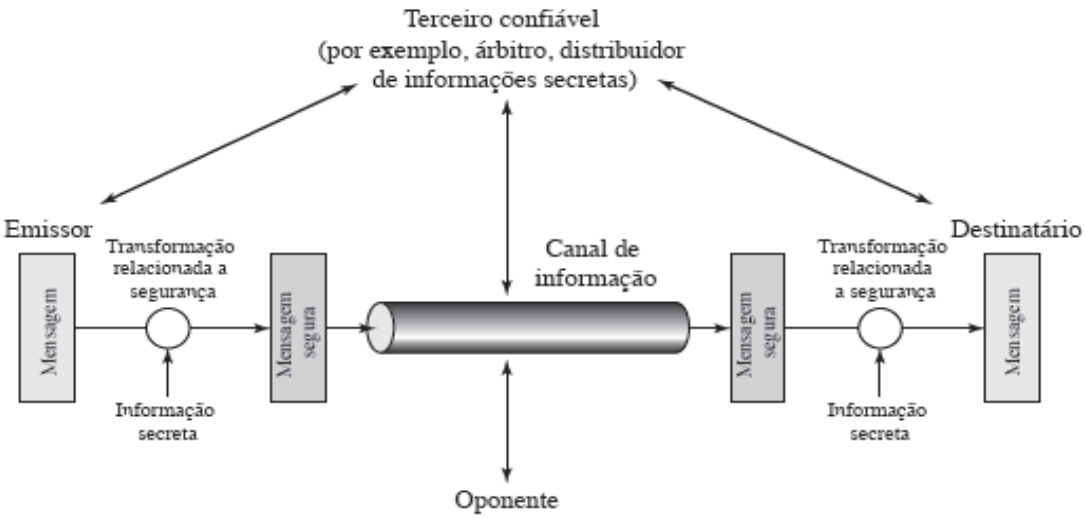
Uma boa Criptografia consegue, até certo ponto, resistir aos ataques que lhe são direcionados. Todavia, existem maneira alternativas de se chegar às informações por descuidos humanos, principalmente com materiais em forma física.

> Uma vez encontrada uma falha de segurança, pode-se consertá-la. Mas encontrar as falhas, para início de conversa, pode ser extremamente difícil. Segurança é diferente de qualquer outro requisito de projeto, porque nele funcionalidade não é igual a qualidade: se um editor de texto imprime corretamente, sabe-se que a função de impressão funciona. Segurança é diferente: só porque um cofre reconhece a combinação correta para abri-lo, não significa que seu conteúdo está seguro contra um chaveiro ou arrombador. Nenhuma quantidade de testes beta revelará todas as falhas de segurança de um sistema, e não haverá nenhum teste possível que prove a ausência destas falhas (REZENDE, 2019, p. 5).

Como dito por Centeno (2018), o objetivo da Criptografia é fazer com que apenas as duas partes (Alice e Bob) 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. Um modelo que define bem como funciona uma cifra é o mostrado no livro Criptografia e Segurança de Redes escrito por Stallings (2015), conforme se pode verificar abaixo.

Centeno (2018), descreve também algumas definições de elementos importantes para a Criptografia, como a mensagem, que se trata da informação que se busca manter desconhecida aos outros com exceção do receptor; o transmissor (Alice), que é o portador da mensagem, o qual irá criptografá-la e a envia ao receptor; o receptor (Bob), que é quem irá receber a mensagem criptografada e deve ser capaz de descriptografar a mensagem, para obter a original, como demonstrado por Stallings na Figura 1; a chave, que são dados aos quais permitem criptografar e descriptografar a mensagem, podendo haver mais de uma chave dependendo do sistema de distribuição de chaves e da cifra utilizada; e a distribuição das chaves, o que permite que o receptor consiga ter acesso à chave para que decifre a mensagem, processo em que se encontram grande parte dos problemas, já que o canal de comunicação usado pode não ser 100% seguro.

Figura 1 - Modelo de segurança de rede.



Fonte: Stallings (2015, p. 17)

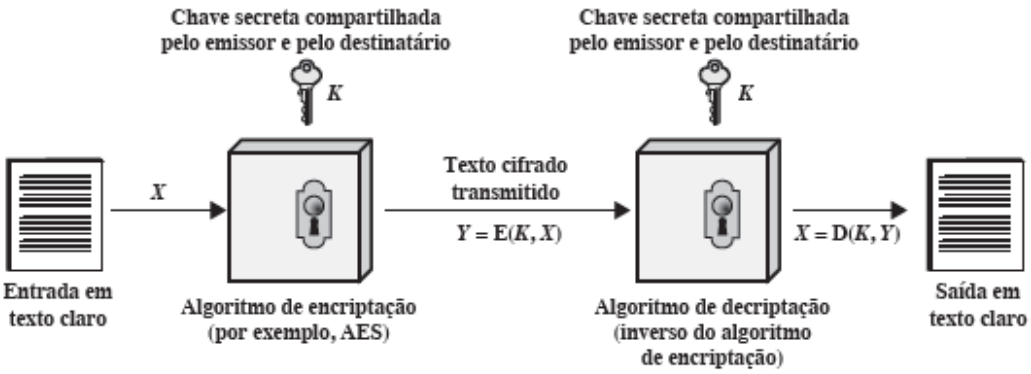
De acordo com Cavalcante (2005), a chave indica o nível de dificuldade que se tem para decodificar a mensagem. O tamanho da chave tem relação exponencial com o trabalho para decodificar, mas também com o trabalho de um agente externo de identificar qual a chave. Os tipos de chave dependem de qual tipo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

Segundo Stallings (2015), a Criptografia simétrica, onde X é a mensagem clara, K é a chave usada e Y é a mensagem criptografada, exemplificado na Figura 2.

Figura 2 – Modelo simplificado da encriptação simétrica.



Fonte: Stallings (2015, p. 21)

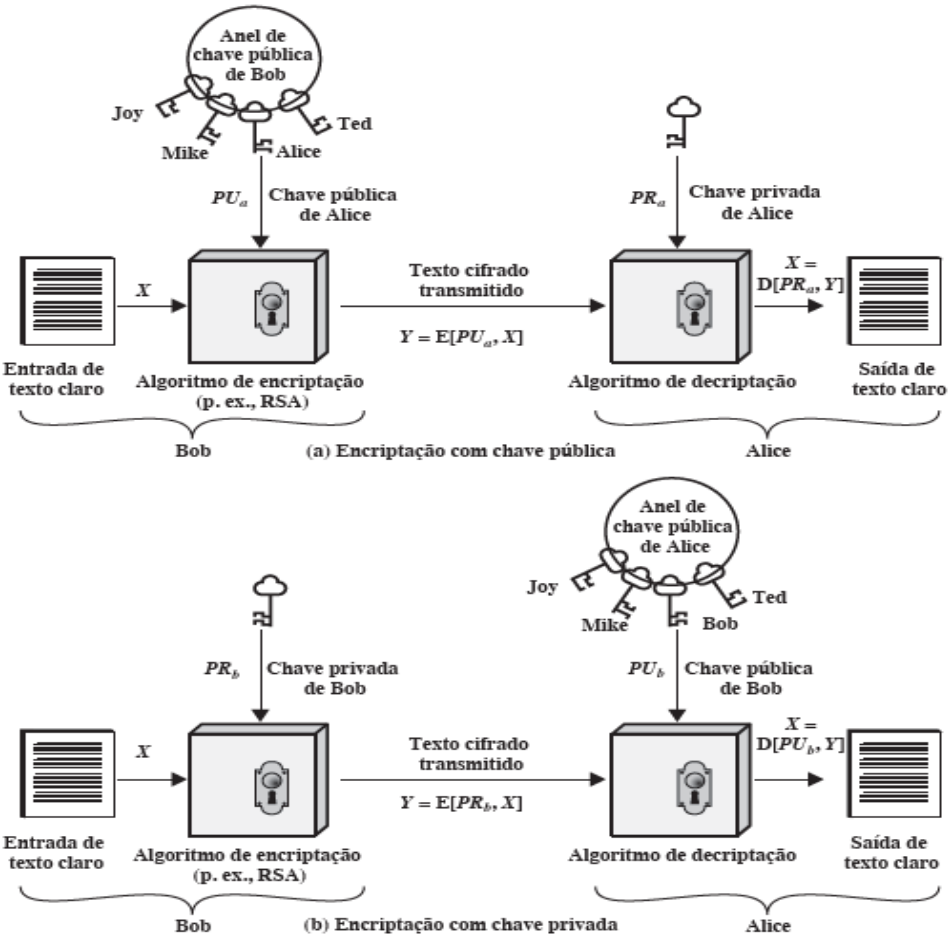
Este modelo de Criptografia atualmente não representa a segurança esperada, porém é um método muito bom quando se necessita de velocidade, visto que ele consegue, com menos recursos, fazer a codificação do texto. É muito usado em canais que não necessitam de grande segurança. Em casos nos quais mais segurança se faz necessária, utiliza-se a Criptografia assimétrica.

A Criptografia assimétrica, segundo Cavalcante (2005), utiliza-se de 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.

O método RSA se tornou famoso pelo fator de dificuldade de fatorar números extensos. O grande tamanho da chave torna o processo muito demorado, assim garantindo a segurança da informação, já que, até o ponto de um invasor decifrar, o

valor da informação já não é o mesmo, podendo já ser praticamente nulo. Observe-se a figura 3.

Figura 3– Criptografia de chave pública.



Fonte: Stallings (2015, p. 202)

O Modelo de Stallings define bem o funcionamento da Criptografia assimétrica, como mostrado na figura, onde X é a mensagem clara, PU é a chave pública, PR é a chave privada e Y é a mensagem cifrada.

Como dito acima, ambos os tipos de criptografia simétrica e assimétrica têm como elemento fundamental de seu funcionamento a chave criptográfica, que deve ser mantida em total segredo em relação a agentes externos.

No próximo capítulo será apresentado um importante protocolo de segurança, com base nas leis da Mecânica Quântica, que contribuirá muito nesse processo de troca segura de chaves.

4 FUNCIONAMENTO DO PROTOCOLO BB84

Como citado por Sobral e Machado (2019), o protocolo BB84 criado por Gilles Brassard e Charles Bennett, em 1984, pioneiro dos protocolos criptográficos para a trocas de chaves, traz um sistema prático baseado nas leis da mecânica quântica, em principal o princípio da incerteza, que permite a comunicação segura entre as partes (Alice e Bob) de maneira segura através de um canal público, a fim de se obter uma chave secreta.

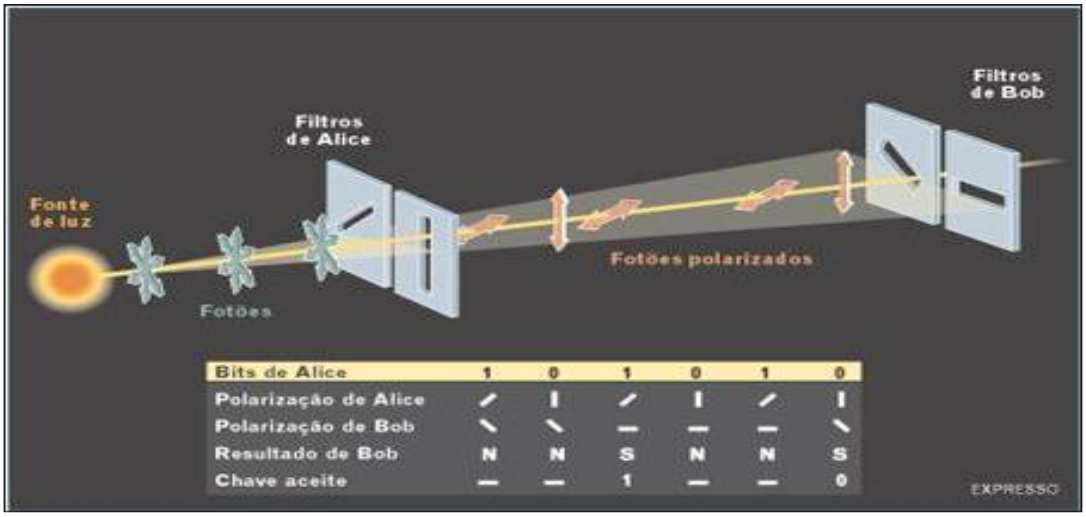
De acordo com López e Lacalle (2005), um dos grandes problemas práticos para se obter uma comunicação protegida é a troca de uma chave segura. Tal troca contribui para o sucesso dos sistemas de chaves públicas, nos quais se permite dispensar a distribuição de uma chave secreta, havendo duas chaves: a 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.

Como descrito por Guedes et al. (2008) a distribuição quântica de chaves utiliza de propriedades da mecânica quântica, de forma a tentar estabelecer o melhor cenário para a troca de chaves, por meio de três propriedades:

> “1. Toda medição perturba o sistema (GISIN et al. 2007);
> 2. Não é possível determinar com 100% de certeza a posição e o momento de uma dada partícula (Princípio da incerteza de Heisenberg) (HEISENBERG, 1927);
> 3. Não é possível medir a polarização de um fóton simultaneamente na base diagonal e retilínea (Teorema da Não-Clonagem) (WOOTERS; ZUREK, 1982);” (GUEDES *et al*., 2008, p.1)

Rigolin e Rieznik (2005) descrevem o protocolo como um utilizador de sistemas quânticos de dois níveis, com os estados |0> e |1> representando fótons linearmente polarizados em direções ortogonais. Como Sobral e Machado (2019, p. 279) citam: “[...] ao trocarem entre suas várias posições disponíveis os fótons vibram e se, num grupo de fótons todos vibram na mesma direção, então eles estão polarizados. [...]”, como mostrado na Figura 4.

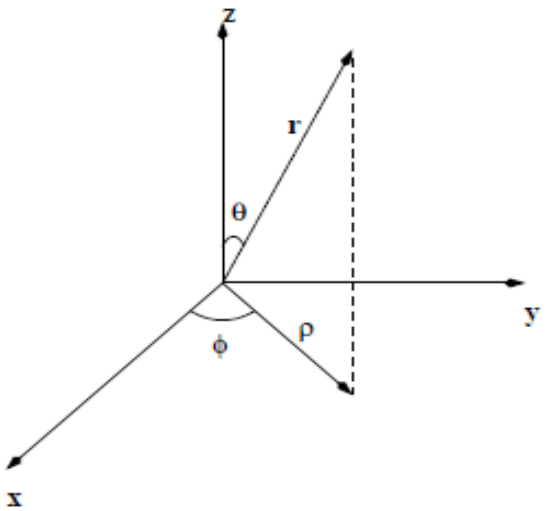
Figura 4 – Polarização de fótons na comunidade Alice e Bob.



Fonte: Sobral e Machado (2019, p. 278).

De acordo com Rigolin e Rieznik (2005, p. 519) “[...]os estados |0> e |1> podem representar fótons que se propagam na direção *z* com campos elétricos oscilando no plano *xy”*, onde as direções de polarização são representadas por vetores unitários, utilizando coordenadas esféricas, como mostrados na Figura 5.

Figura 5 – Coordenadas esféricas.

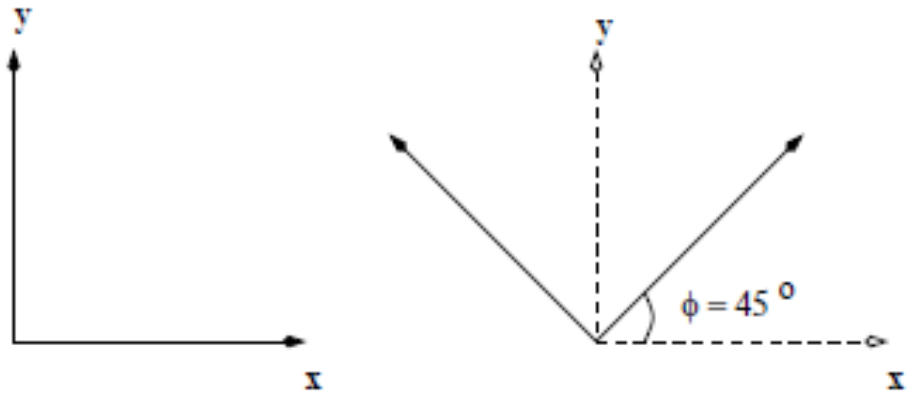


Fonte: Rigolin e Rieznik (2005, p. 519).

Marquezino (2003) explica que se utiliza de dois parâmetros (ângulos) para especificação das bases a serem usadas para transmissão e recepção dos fótons. Normalmente, utilizam-se duas bases recomendadas para os dois tipos de

polarização que o protocolo necessita: a base retilínea (+), onde os fótons podem ser polarizados em 0 ou 90 graus; ou a base diagonal (x), onde se pode fazer a polarização em 45 ou 135 graus, como bem se exemplifica na Figura 6, que mostra o ângulo das duas bases.

Figura 6 – Representação das bases A e B.



Fonte: Rigolin e Rieznik (2005, p. 519).

Vale lembrar que, como dito por Sobral e Machado (2019), pode-se substituir uma das bases pela base circular com a mão direita e esquerda, seguindo a regra da mão direita.

Construiu-se um quadro exemplo para as bases, de forma finalizada, conforme mostra o quadro 3.

Quadro 3 – Valor das bases de acordo com a polarização

Base	Grau (°)	Valor
+	0°	1
+	90°	0
X	45°	1
X	135°	0

Fonte: Próprio autor (2020)

Rigolin e Rieznik (2005) descrevem que, após combinados os estados de polarização que servem como base, Alice deve escolher uma sequência aleatória de bits que serão enviados e escolher qual base será usada para cada bit, aplicá-la nos

bits e enviá-los a Bob. Este, por sua vez, deve selecionar aleatoriamente qual base utilizará para detectar os fótons. Como exemplo utilizaremos os bits 110001 como os bits e “aababa” como as bases escolhidas por Alice, então a sequência de fótons enviada seria: |1>a, |1>a, |0>b, |0>a, |0>b, |1>a.

Após a detecção dos fótons por Bob, ambos devem revelar publicamente, no canal, as bases usadas para enviar e detectar cada fóton, porém não são revelados os bits enviados nem aqueles resultantes das medidas. Os bits enviados e detectados com bases diferentes são retirados da sequência. Consideram-se, assim, apenas os resultados com as mesmas bases. Em seguida, revela-se uma parte dos resultados. Nesta etapa, normalmente se reduz a quantidade para uma média de 50% dos bits iniciais. Apesar de 75% estar correta, apenas 50% representam informação, sendo o restante normalmente a parte revelada para conferir os resultados.

Caso os bits não tenham sido monitorados, os resultados de Alice e Bob devem ser iguais. Se os dados revelados publicamente coincidirem, isso serve como prova de que os bits não foram monitorados. Os bits restantes ainda não revelados serão os dados da chave. O quadro 4, mostrado por Rigolin e Rieznik (2005), representa um caso de transmissão de chave, considerando uma situação em que alguns fótons podem se perder de maneira bem geral.

Quadro 4 – Sequência da transmissão quântica entre Alice e Bob.

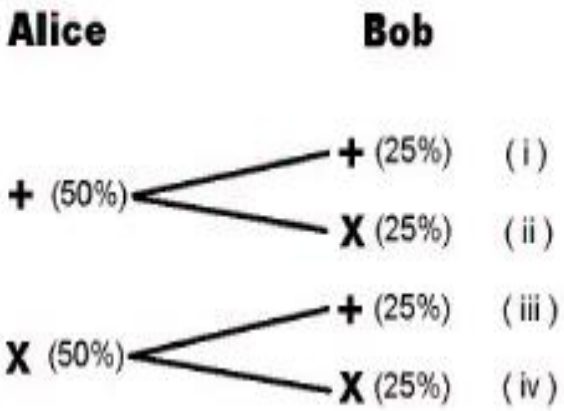
Sequência de bits de Alice	0	1	1	0	1	1	0	0	1
Bases escolhidas por Alice	B	A	B	A	A	A	A	A	B
Fótons enviados por Alice	|0>b	|1>a	|1>b	|0>a	|1>a	|1>a	|0>a	|0>a	|1>b
Bases escolhidas por Bob	A	B	B	A	A	B	B	A	B
Bits recebidos por Bob	1		1		1	0	0	0	
Bob informa fótons	A		B		A	B	B	A	
Alice informa corretas			ok		ok			ok	
Informação Compartilhada			1		1			0	
Bob revela alguns bits					1				
Alice confirma				ok					
Chave			1						

Fonte: Rigolin e Rieznik (2005, p. 519).

De acordo com Marquezino (2003), o protocolo traz certas vantagens, principalmente no que diz respeito aos ataques possíveis atualmente. Um deles é o *man-in-middle,* em relação ao qual será mostrado como o protocolo consegue identificar a presença desse agente que busca capturar dados. Chamou-se esse agente de Eve. Seguindo o princípio da não-clonagem, logo que Eve intercepta os q-bits enviados por Alice e os copia, isso já afeta todo o sistema, fazendo com que os resultados de Bob sejam completamente aleatórios. Então, ainda existem duas maneiras de se ler os q-bits interceptados: interceptar e reenviar; ou aplicar uma medição de uma base intermediária, conforme será discutido a seguir.

A estratégia de interceptar e reenviar consiste em Eve interceptar os q-bits vindos de Alice, medi-los escolhendo uma das bases aleatoriamente e, após isso, os reenviar para Bob. Em um caso em que não há a ação de Eve, a chance das chaves pode ser definida pela Figura 7.

Figura 7 – Casos possíveis no BB84 sem espionagem.

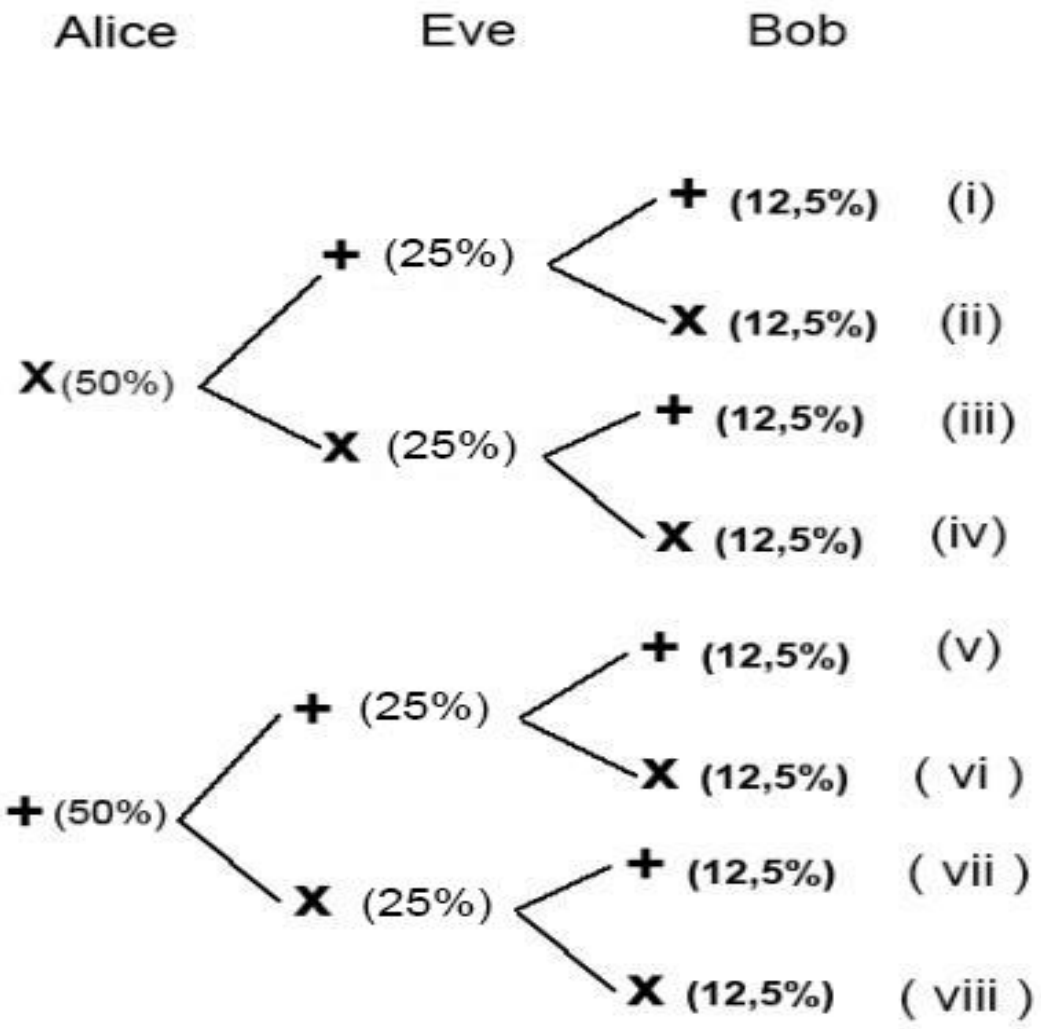


Fonte: Marquezino (2003, p. 10).

Reforçando o dito por Marquezino (2003, p.10), “na reconciliação de bases, Alice e Bob irão concordar somente nos casos (i) e (iv), onde ambos usam a mesma base. Em (ii) e (iii) metade dos bits estarão corretos, mas, mesmo assim, serão descartados, pois a informação é aleatória”.

No caso da medição feita por Eve, se adiciona uma coluna a mais na distribuição de porcentagens de chance de acerto, o que reduz a chance de porcentagem do acerto de Bob, como mostrado na Figura 8.

Figura 8 – Casos possíveis no BB84 com espionagem.

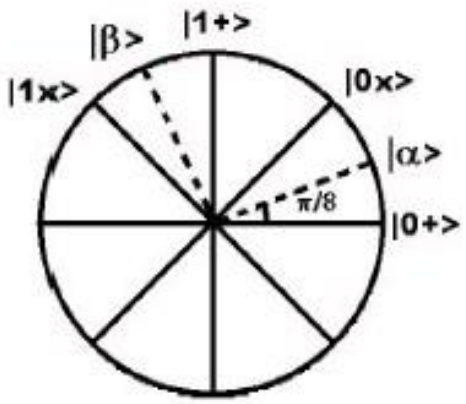


Fonte: Marquezino (2003, p. 10).

Portanto nessa estratégia Eve obtém 50% da informação, mas introduz uma taxa de erro de 25%, o que se mostra claro quando comparados os resultados de algumas bases, assim fazendo com que o processo recomece. Eve também poderia aplicar a estratégia em alguns fótons, para que a perturbação gerada fosse menor, podendo ser confundida com um ruído. No entanto, a informação descoberta decai junto e Alice e Bob poderiam evitar esse problema, utilizando algum método de amplificação de privacidade.

Outra estratégia seria a de base intermediária, onde Eve mede sempre em uma mesma base, sendo essa diferente das outras duas mencionadas, utilizando de uma base intermediária, que Marquezino (2003) exibe na Figura 9, considerando que |α> representa 0 e |β> representa 1.

Figura 9 – Base intermediária.



Fonte: Marquezino (2003, p. 10).

Porém essa técnica não apresenta vantagem em comparação a anterior, já que, calculando as chances de Eve acertar o valor enviado por Alice através dessa base intermediária, tem-se aproximadamente 0.854. Calculando a probabilidade de Bob obter um resultado incorreto, mesmo com a utilização da base correta no q-bit produzido por Eve, o resultado é de 0.25.

Mesmo essa estratégia parecendo mais eficiente, com uma probabilidade maior de acertar a medição, o ganho de informação por bit da chave se revela em aproximadamente 0.399.

Isso leva ao conceito da entropia de Shannon, um conceito da Teoria da Informação que serve para medir a quantidade de informação ganha ao medir esse sistema. Um ganho menor não traz vantagens para Eve sobre a estratégia de interceptar e reenviar.

4.1. APLICAÇÃO DE FUNCIONALIDADE E PROBLEMAS PRÁTICOS

O protocolo quando aplicado em um sistema considerado perfeito, ou seja, onde Alice e Bob possuam equipamentos perfeitos, a comunicação ocorre sem

nenhum ruído no canal e o emissor é capaz de enviar um único fóton por vez. Como dito por Marquezino (2003), nesse contexto o protocolo funciona com um nível de segurança praticamente absoluta e se mostra de grande eficiência, podendo ser aplicado a muitas cifras criptográficas atuais. Muitos, como o próprio Marquezino (2003), recomendam sua utilização com a cifra de Vernam.

Como afirma Tixaire (2007), apesar da segurança teoricamente perfeita da Criptografia quântica, ainda é necessária sua implementação, para que *crackers* quânticos tenham acesso ao sistema e seja possível encontrar lacunas que podem ainda não ter sido idealizadas. A partir daí, podem ser feitos implementos de melhorias no protocolo visto que não estão disponíveis sistemas funcionais e constantemente ativos para que sejam atacados e explorados.

A aplicação teórica do protocolo BB84 pode trazer a impressão de que o protocolo já está pronto para a aplicação, porém as restrições requeridas por ele, em contexto prático, são muito difíceis de serem satisfeitas. Como explicado por Marquezino (2003), em situações concretas, nos deparamos com diversas condições não ideais, como ruídos no canal, equipamentos imperfeitos e limitações dos próprios equipamentos.

Bennett *et. Al.* (1992), em artigo publicado no *Journal of Cryptology*, revelam resultados do primeiro teste de aplicação do protocolo. Identificaram-se dois problemas que tornavam sua prática inadequada. O primeiro é que os detectores possuem um nível de ruído, mesmo em um cenário com ausência de um interceptador; o segundo é a dificuldade de se produzir um pulso de luz que possui apenas um fóton. É muito mais fácil produzir um pulso que contenha diversos fótons, o que permite que um interceptador possa dividir o pulso em dois ou mais fótons para que seja feita a leitura de um e o envio do outro.

Como citado por Sobral e Machado (2019), a Criptografia quântica, hoje, está além da teoria. Diversos laboratórios já a realizaram sua implementação. Existem redes sendo planejadas e construídas por empresas, nas quais ainda se tenta reduzir o fluxo de fótons enviados para apenas um. Busca-se, ainda, utilizar canais quânticos que tragam menor interferências aos fótons.

Ambos os canais de comunicação trazem dificuldades de envio. Tanto a transmissão de fótons pelo ar, que pode sofrer interferências causadas por mudanças climáticas, quanto aquela realizada por meio de fibras óticas, material que demanda nível de pureza muito elevado para que seja feita a comunicação. Mesmo com níveis

de limpidez ideias, grandes distâncias fazem aumentar a taxa de erros, devido ao Princípio da Incerteza de Heisenberg. Uma opção que já é cogitada é a de um retransmissor quântico para que se possa aumentar a distância percorrida pelos fótons sem que ocorra alteração ou perda.

Marquezino (2003) afirma que o meio mais comum usado como canal de comunicação é a fibra, visto que sua implementação e controle conseguem ser mais estáveis em comparação à transmissão feita pelo ar, que sofre mais interferências.

Junto com a utilização da fibra, Marquezino (2003) diz que se deve escolher o comprimento de onda dos fótons que serão utilizados para o envio, a fim de que se tenha compatibilidade entrar o emissor e o receptor. Para essa situação, de acordo com o autor, existem duas opções: fótons com 800 nm ou utilizar a faixa de 1300 até 1500 nm.

No primeiro caso, a vantagem encontrada é a compatibilidade com os contadores de fótons existentes no mercado, gerando facilidade na sua recepção e contagem; porém a desvantagem está na necessidade de utilização de tipos de fibra especiais, já que os tipos mais comuns não são compatíveis com essa frequência de onda. Essa frequência chega a ter um ponto de atenuação de 2 dB/km, que é considerado alto em comparação com a outra alternativa. Na segunda opção, ocorre o contrário. A frequência é compatível com os modelos de fibra ótica mais comuns e sua atenuação é de baixa escala, variando de 0.20 dB/km até 0.35 dB/km, porém é necessário que sejam desenvolvidos contadores de fótons para esses tipos de frequência.

Sobral e Machado (2019) citam, ainda, sobre a criação de fontes de fótons de tamanho reduzido e baixo custo, processo que encontra, também, dificuldades de implementação, uma vez que se faz necessária a integração da infraestrutura da rede quântica à da rede atual.

4.2. TESTES E POSSIBILIDADES

Como anteriormente citado, diversos testes foram feitos em laboratório a fim de alcançar um ponto próximo de uma futura prática. A IBM realizou a primeira experiência nesse sentido em 1992, conforme salientado por Marquezino (2003),

utilizando uma distância de apenas 30 centímetros. Mesmo diante da distância diminuta, o resultado foi de grande importância.

Como citam Bennett *et. Al.* (1992), o experimento foi realizado por um aparelho criado pelos autores do artigo. Esse dispositivo fazia a transmissão dos feixes, desde a criação do flash de luz, polarização, envio através de um caminho óptico de ar livre de 32 centímetros e a detecção junto à conversão de polarização. O funcionamento ocorria sob o controle de um computador da IBM, citado apenas como IBM PC, que continha as representações de dois softwares separados. Um funcionava como remetente, representando Alice, que controlava a parte de envio do aparelho; e outro, que controlava o receptor, representando Bob. Havia também uma terceira opção, que funcionava como interceptador, representando Eve. Porém, o programa Eve funcionava por meio de simulação, sem sua parte experimental anexada ao aparelho.

Mesmo os programas estando neste mesmo computador, IBM PC, suas comunicações eram restritas, não permitindo nenhuma comunicação direta entre o software de Alice e o software de Bob, com exceção de um canal público, como é exigido pelo protocolo. A escolha da base de polarização de leitura por Bob também era feita de maneira aleatória, por meio de um grande arquivo de bits aleatórios retirados pelo computador de um disquete, onde anteriormente já havia ocorrido a seleção de bits aleatórios de um dos fotomultiplicadores, iluminado por um LED auxiliar.

De acordo com os autores, o experimento ainda era um protótipo. Em um cenário mais realista, a taxa de erro poderia ser corrigida pelo alinhamento ótico e resfriamento dos fotomultiplicadores, entretanto seria necessário um canal mais longo, uma vez que o ruído, a eficiência dos detectores e o canal atravessado poderiam ser grandes problemas a ainda serem combatidos.

Marquezino (2003) segue explicando que, quando se trata da prática aplicável em relação a transmissões de dados, é visada uma distância muito maior, que chegue à proporção de quilômetros, ou distâncias que sejam muito inferiores a 30 centímetros, realidade definida pelo autor como “não muito óbvia” (MARQEUZINO, 2003, p. 13), porém verificável em casos de aproximação, como e o caso do uso de cartões de crédito que necessitam acercar-se da máquina para que se efetive a troca de dados. Esse experimento da IBM, mesmo não trazendo as melhores proporções, constitui um grande marco para a aplicação do protocolo, visto que foi o primeiro teste efetivo e funcional divulgado para a comunidade científica.

Gisin *et al.* (2002) complementam a explicação de Marquezino citando que, depois desse primeiro experimento realizado na IBM, diversos outros foram conduzidos por mais alguns anos, porém grande parte, senão quase todos, em laboratórios ou equipamentos de laboratórios.

Marquezino (2003) conclui dizendo que nos dias mais atuais já se conseguem fazer essas comunicações em meios de algumas dezenas de quilômetros, sem que haja grandes ruídos no canal, como demonstra um experimento realizado na Suíça em 2002. Neste procedimento, conduzido por Gisin *et al.* (2002), buscava-se a troca de chaves, ligando dois pontos que estavam a 67 quilômetros de distância. O experimento se deu com um protótipo de distribuição de chaves quânticas, tendo Alice e Bob representados por duas caixas de 10 polegadas, ligadas por fibra ótica. O teste teve como foco testar a estabilidade do sistema plug & play autocompensador criado por Muller *et al*. (1997) no artigo *Plug&play systems for quantum cryptograph*y, através de cabos terrestres e aéreos.

Embora os testes citados realizem apenas a geração das chaves criptográficas, foco do protocolo, outro aspecto a se considerar diante de sua aplicação é a segurança da cifra a ser utilizada.

Como recomendado por Marquezino (2003), a cifra de Vernam, sobre a qual trata o próximo capítulo, é uma boa opção de aplicação junto ao protocolo BB84, uma vez que já se comprovou sua confiabilidade e segurança, pois acrescenta um elevado nível criptográfico de proteção das mensagens.

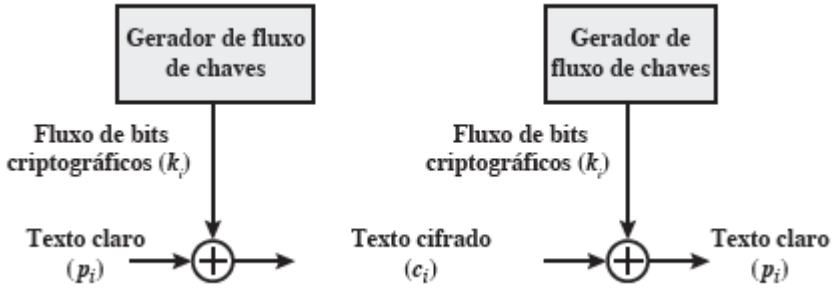
5 BREVE EXPLICAÇÃO SOBRE A CIFRA DE VERNAM

Como descrito por Stallings (2015, p. 35) em seu livro Criptografia e Segurança de Redes de Computadores Princípios e Práticas menciona que “a principal defesa contra a técnica criptoanalítica descrita é escolher uma palavra-chave que seja tão longa quanto o texto claro [...]”. Esse sistema foi introduzido por um engenheiro da AT&T, chamado Gilbert Vernam. Em 1918, Vernam traz um sistema criptográfico que funciona por meio de bits no lugar das letras, muito comuns na época. Ocorre a entrada de um texto nomeado de (Pi), em conjunto com uma chave nomeada (k) para que o texto seja cifrado, usando-se a operação XOR bit a bit. Para realizar a decriptação, repete-se a operação. O processo da cifra de Vernam descrito acima é mostrado na figura 10.

Fiarresga (2010) explica que para que seja enviada a mensagem através da cifra de Vernam é necessário que o receptor e o transmissor possuam a chave. A chave deve ser aleatória e conter, no mínimo, o mesmo tamanho da mensagem.

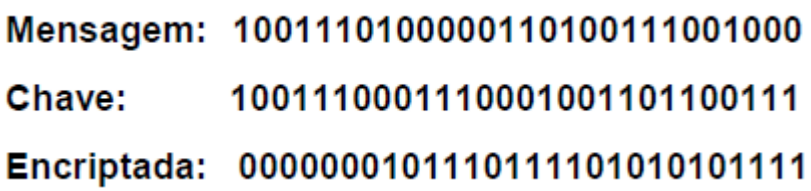
Então a encriptação bit a bit é feita de maneira que cada bit gerado da mensagem (Pi) efetue a operação de XOR, com um bit pertencente à chave (k). Assim, a divisão da mensagem é enumerada em uma ordem, X = (X1, X2, ..., Xn), e a chave também segue o mesmo processo, K = (K1, K2, ..., Kn). Então, é efetuado o processo de XOR, ocorrendo a encriptação da seguinte forma: (Y = X + K) = (Y1 = X1 + K1; Y2 = X2 + K2, ..., Yn = Xn + Yn). A figura 11 demonstra um exemplo do funcionamento da cifra de maneira prática.

Figura 10 – Cifra de Vernam.



Fonte: Stallings (2005, p. 35)

Figura 11– Funcionamento da Cifra de Vernam.



Fonte: Fiarresga (2010, p. 115)

Vernam propõe para a cifra uma palavra-passe muito extensa, mas eventualmente ocorria sua repetição e, nas palavras de Stallings (2015, p. 36) “embora esse esquema com uma chave longa apresenta dificuldades de criptoanálise formidáveis, ele pode ser quebrado com um número suficiente de texto cifrado, com o uso de sequências de texto claro conhecidas ou prováveis, ou ambos”.

Como Stallings (2015) afirma, Joseph Mauborgne, um oficial do exército do Estados Unidos, trouxe uma melhoria na cifra que aumenta a segurança, com a utilização de uma chave aleatória que fosse tão grande quanto a mensagem, de maneira que a chave não se repita. Essa evolução incluía o fato de que a chave deveria ser utilizada para encriptar e decriptar uma única mensagem e, após isso, ser descartada.

De acordo com Fiarresga (2010), esse método se torna muito efetivo para proteção, configurando uma Criptografia de alto nível, utilizada até em âmbito militar. Seu nome, *One-Time Pad*, foi dado pela ideia de se empregar apenas uma vez cada chave.

5.1. A CIFRA ASSOCIADA AO PROTOCOLO BB84

Como Marquezino (2003) discute, mesmo com a melhoria trazida por Mauborgne, o One-Time Pad, Stallings (2015), 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) explica 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””[3] (TIXAIRE, 2007, p. 1, tradução nossa)[4], 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 já que, como mostrado anteriormente no capítulo 4, um espião não consegue extrair informações sem que seja revelada sua presença aos que estão trocando as mensagens, através do 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 ” el método Vernam o clave de “un solo uso””

6 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. 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 a máquina do autor, fazendo o papel de receptor, que operou no sistema operacional Windows 7. Como emissor, utilizou-se uma máquina virtualizada dentro do ambiente do autor, que também operou no sistema operacional Windows 7.

O protocolo foi dividido em seis fases para melhor adequação às explicações. 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 feitas pelo autor, 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, o autor escolheu os 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 12.

Figura 12 - Emissor criando a entrada polarizada.

Fonte: Próprio autor (2020)

Após 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 13, 14 e 15.

Figura 13 - Emissor enviando a entrada polarizada.

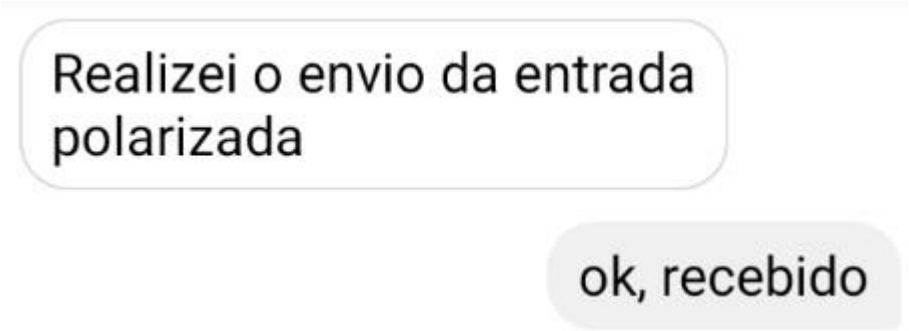
Fonte: Próprio autor (2020)

Figura 14 - Receptor recebendo a entrada polarizada.

Fonte: Próprio autor (2020)

A figura 15 ilustra a comunicação via chat entre o emissor (lado esquerdo) e o receptor (lado direito).

Figura 15 - Mensagem no chat entre ambos.



Fonte: Próprio autor (2020)

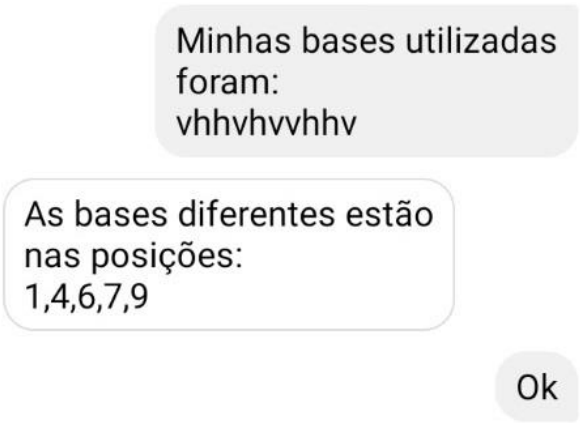
Durante a fase 3, o receptor informa a chave polarizada que recebeu do emissor, no caso “1100011101”, e realiza a inserção da sequência de bases escolhidas por ele (“vhhvhvvhhv”). O receptor recebe, então, o resultado da operação XOR feita novamente (Figura 16).

Figura 16 - Receptor inserindo a entrada polarizada e as bases.

Fonte: Próprio autor (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 17, em que o emissor informa que as bases diferentes estão nas posições 1, 4, 6, 7 e 9.

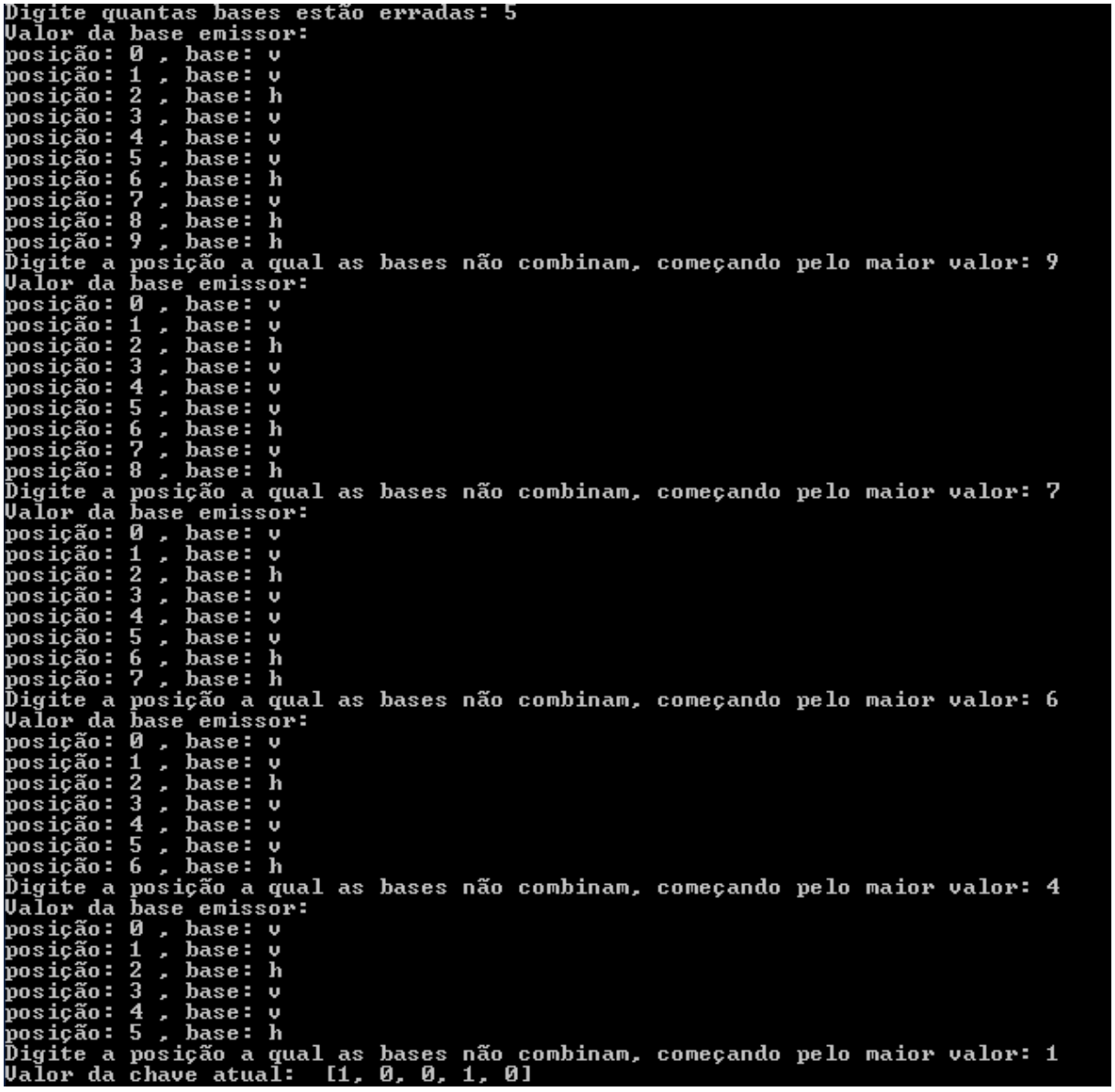
Figura 17 - Receptor envia as bases no chat e recebe as posições que estão diferentes.



Fonte: Próprio autor (2020)

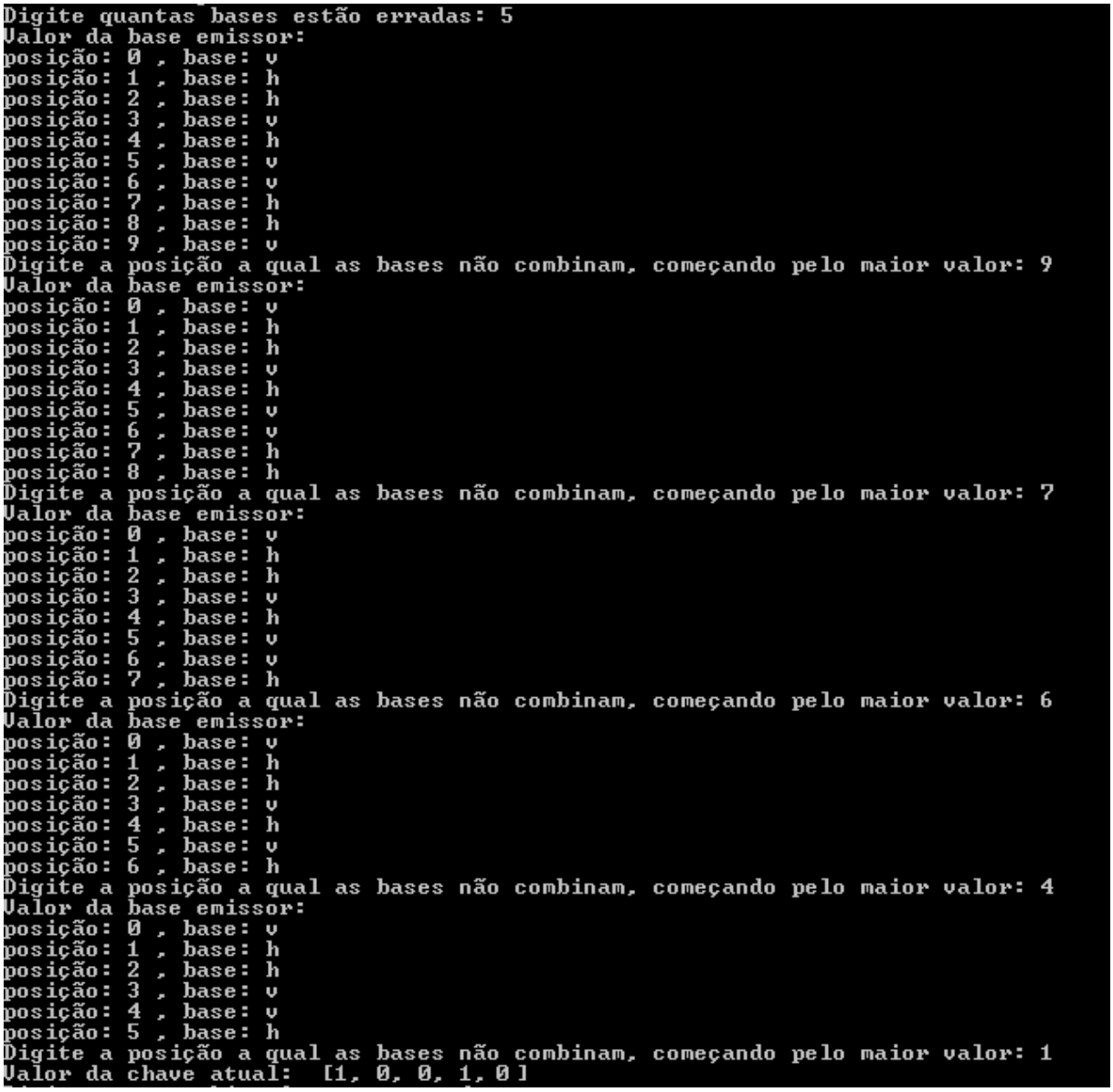
Após isso, ambos informam a quantidade e, em seguida, as bases a serem retiradas da sequência (Figuras 18 e 19).

Figura 18 - Emissor retirando as bases da sequência.



Fonte: Próprio autor (2020)

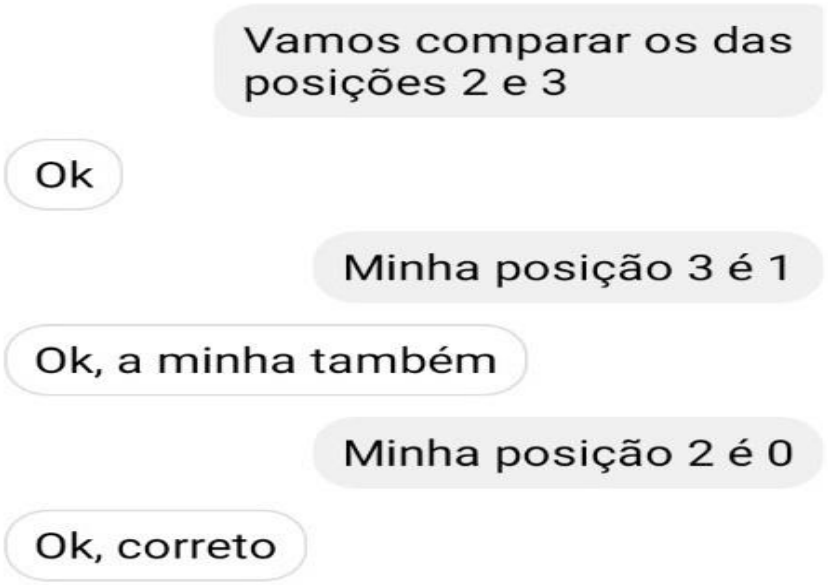
Figura 19 - Receptor retirando as bases da sequência.



Fonte: Próprio autor (2020)

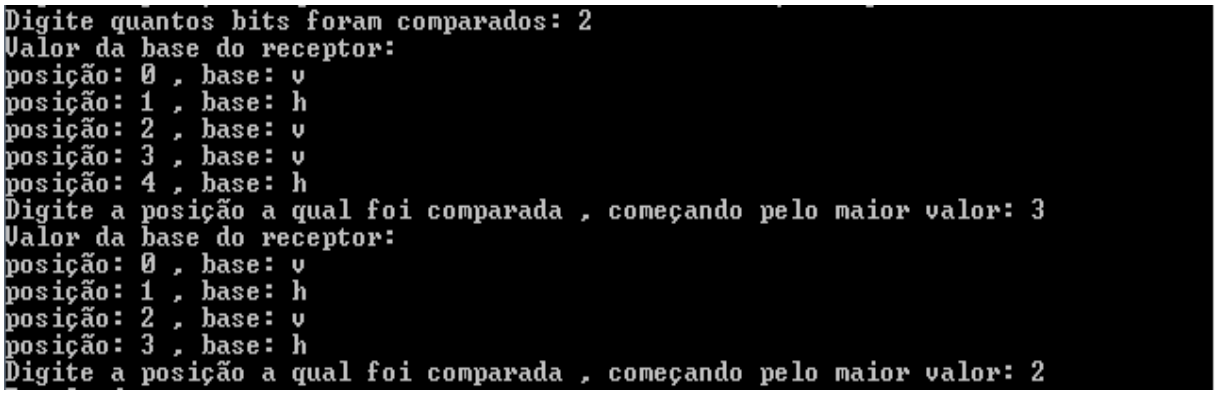
Então, se inicia a fase 5, em que o receptor escolhe alguns bits para serem comparados do valor retornado como chave atual. Na demonstração, são escolhidos dois bits (os das posições 2 e 3), considerando que as posições iniciam no zero. Os bits são comparados via chat (Figura 20) e, após isso, são informadas as posições que foram comparadas para que se retirem da chave final (Figuras 21 e 22).

Figura 20 - Comparação feita no chat.



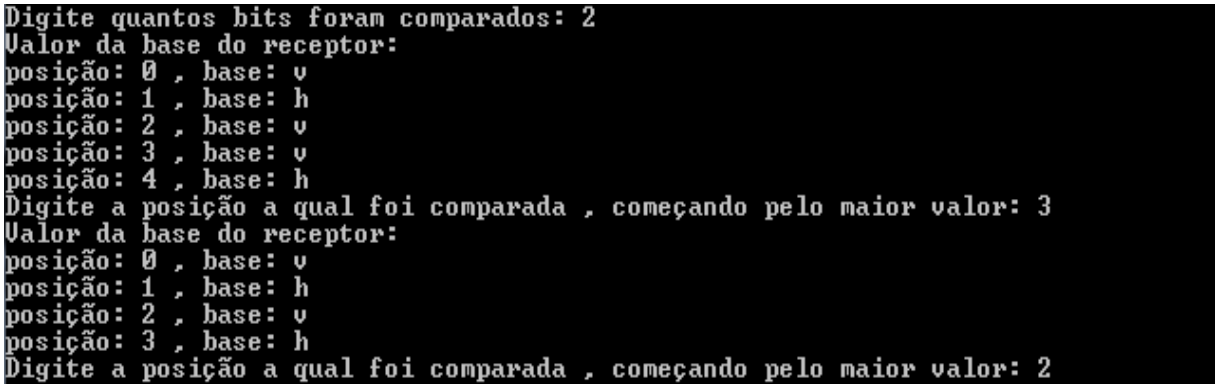
Fonte: Próprio autor (2020)

Figura 21 - Emissor retirando as posições.



Fonte: Próprio autor (2020)

Figura 22 - Receptor retirando as posições.



Fonte: Próprio autor (2020)

Finalizando, na Fase 6, o emissor e o receptor recebem o tamanho da chave final e sua sequência (figuras 23 e 24). O receptor confirma via chat o tamanho da chave com o emissor (figura 25).

Figura 23 - Emissor recebendo o tamanho e valor da chave.

```
Resultados:
Tamanho final da chave 3
Chave final:  [1, 0, 0]
Pressione qualquer tecla para continuar. . .
```

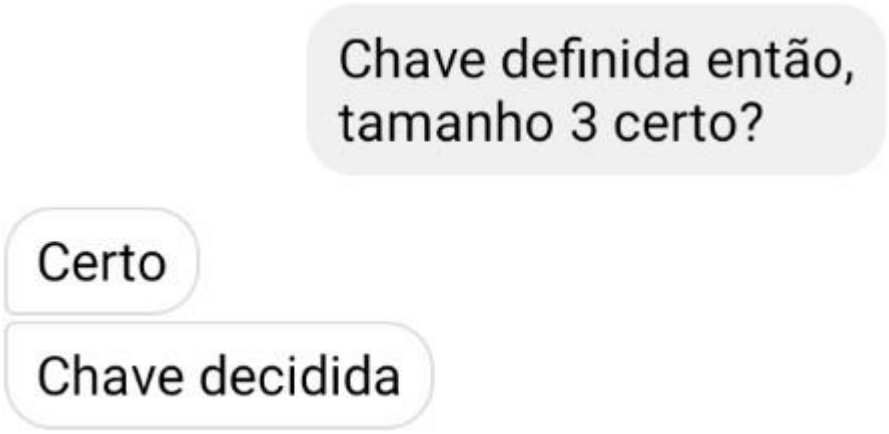
Fonte: Próprio autor (2020)

Figura 24 - Receptor recebendo o tamanho e valor da chave.

```
Digite a posição a qual foi comparada , começando pelo maior valor: 2
Resultados:
Tamanho final da chave 3
Chave final:  [1, 0, 0]
Pressione qualquer tecla para continuar. . .
```

Fonte: Próprio autor (2020)

Figura 25 - Confirmação do tamanho da chave via mensagem.



Fonte: Próprio autor (2020)

7 CONSIDERAÇÕES FINAIS

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.

Mesmo diante de sua eficiência, outros pontos que dificultam a aplicação são o tempo e o trabalho manual, descritos pelos criadores. 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.

Outro caminho a se seguir, como pesquisa futura, seria encontrar outras maneiras de se efetuar a confirmação de identidade de receptor e emissor, uma

espécie de prática externa ou interna ao sistema, em um processo de verificação que seja viável e seguro, sem interferência de um mediador.

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.

8 REFERÊNCIAS

BARBOSA, L. D. A., CORNELISSEN, M. G. Cifra de Hill: uma aplicação aos estudos de matrizes. **Revista Ciências Exatas e Naturais**. p. 152-167, 2017.

BENNET, C. H., BESSETTE, F., BRASSARD, G., SALVAIL, L., SMOLIN, J. *Experimental Quantum Cryptography.* ***Journal of Cryptology***, Vol. 5, p. 3-28, 1992.

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.

BIANCHETTI, T., SAÚGO, C., ORO, N. T. **Criptografia: da história até a aplicação do método RSA**. In IV Jornada Nacional de Educação Matemática e XVII Jornada Regional de Educação Matemática. Resumo – Universidade de Passo fundo, Passo Fundo – Brasil, 2012.

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 Cuátca***. 44 páginas. TCC – Universidade de Sevilla, 2018.

DEUTSCH, D. *Quantum Computational Networks.* ***Royal Society of London Proceedings Series A***, p. 73–90, 1989.

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

GISIN, N., BRENDEL, J., GAUTIER, J-D., GISIN, B., HUNTTNER, B., RIBORDY, G., TITTEL, W., ZBINDEN, H. ***Quantum cryptography and Long Distance Bell Experiments: How to control Decoherence.*** Universidade de Geneva, 2002.

GUEDES, E. B. ISIDRO, C. R. G., LULA JR., B., FECHINE, J. M. **Fundamentos da Distribuição Quântica de Chaves.** Universidade Federal de Campina Grande Campina Grande – Brasil, 2008.

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.

IKRAM, J., MOHSEM, M. *FPGA Iplementation of the BB84 Protocol.* ***Internacional Journal of Computer and Information Engeneering***, Vol.12, P918-921, 2018.

KAHN, D. ***The Codebreakres.*** *The New American Library, Inc*. 1973.

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.

MULLER, A., HERZOG, T., HUTTNER, B., TITTEL, W., ZBINDEN, H., GISIN N.. ***"Plug and play" Systems for Quantum Cryptography.*** Universidade de Geneva 1997.

REZENDE, P. A. D. **Criptografia e Segurança na informática.** 35 páginas. TCC – Universidade de Brasília, Brasília, 2019.

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.

STALLINGS, W. **Criptografia e Segurança em Redes.** 6ª Edição. São Paulo: Pearson Education do Brasil, 2015.

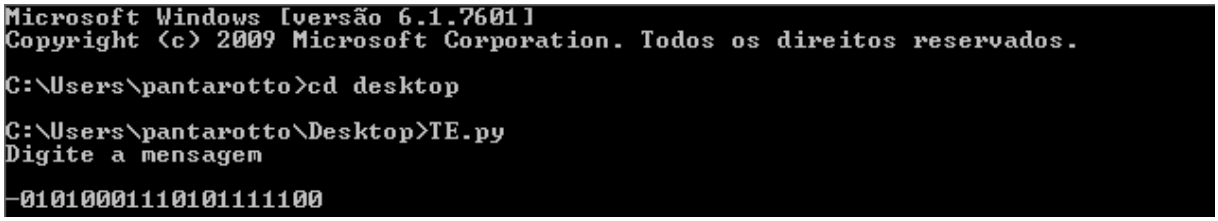
TIXAIRE, A. G. *El Arte de Disfrazar la Información: De la C a la Q.* ***Revista E. Acad. Cienc. Exact. Fís. Nat****.* Vol. 101, p. 307-320, 2007.

APENDICE A – SIMULAÇÂO DO FUNCIONAMENTO COM ENTRADA DE 20 CARACTERES

Figura 1 - Emissor criando a entrada polarizada.

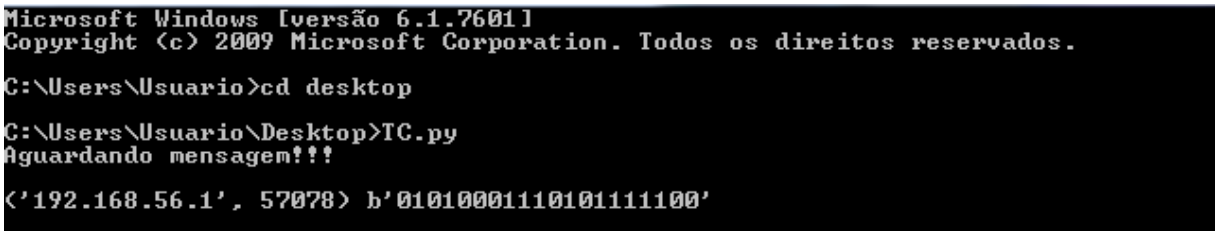
Fonte: Próprio autor (2020)

Figura 2 - Emissor enviando a entrada polarizada.



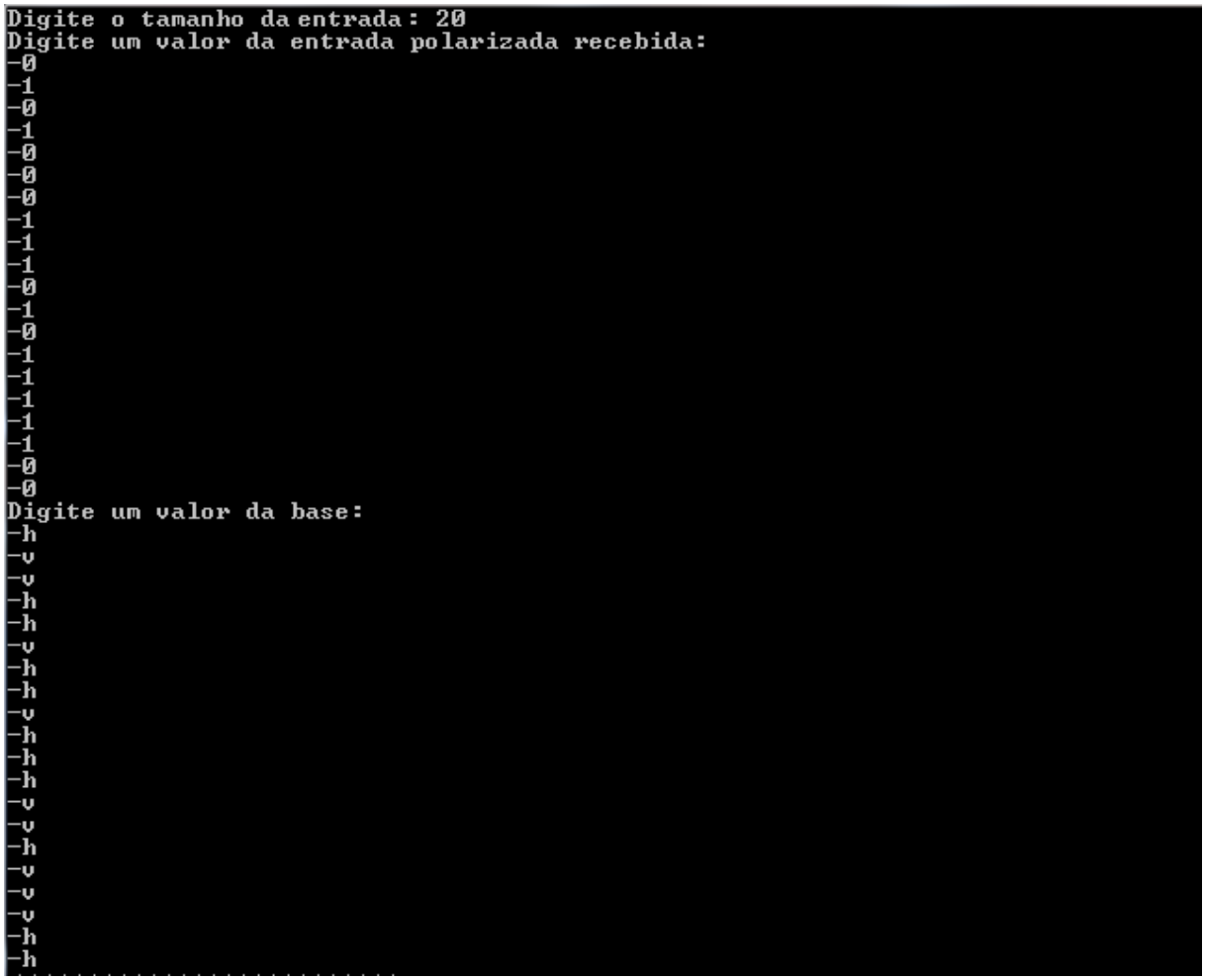
F Fonte: Próprio autor (2020)

Figura 3 - Receptor recebendo a entrada polarizada.



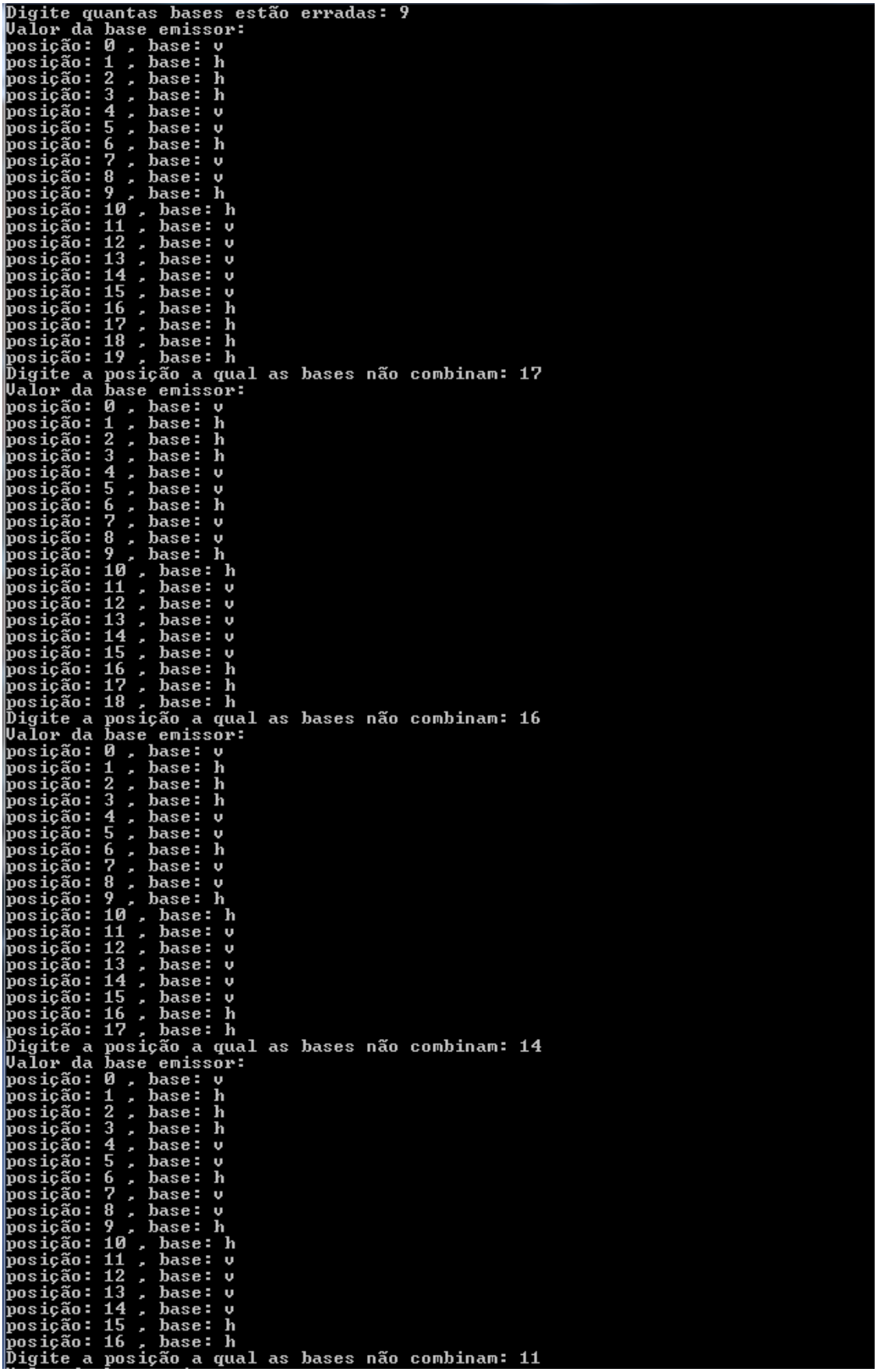
Fonte: Próprio autor (2020)

Figura 4 - Receptor inserindo a entrada polarizada e as bases.



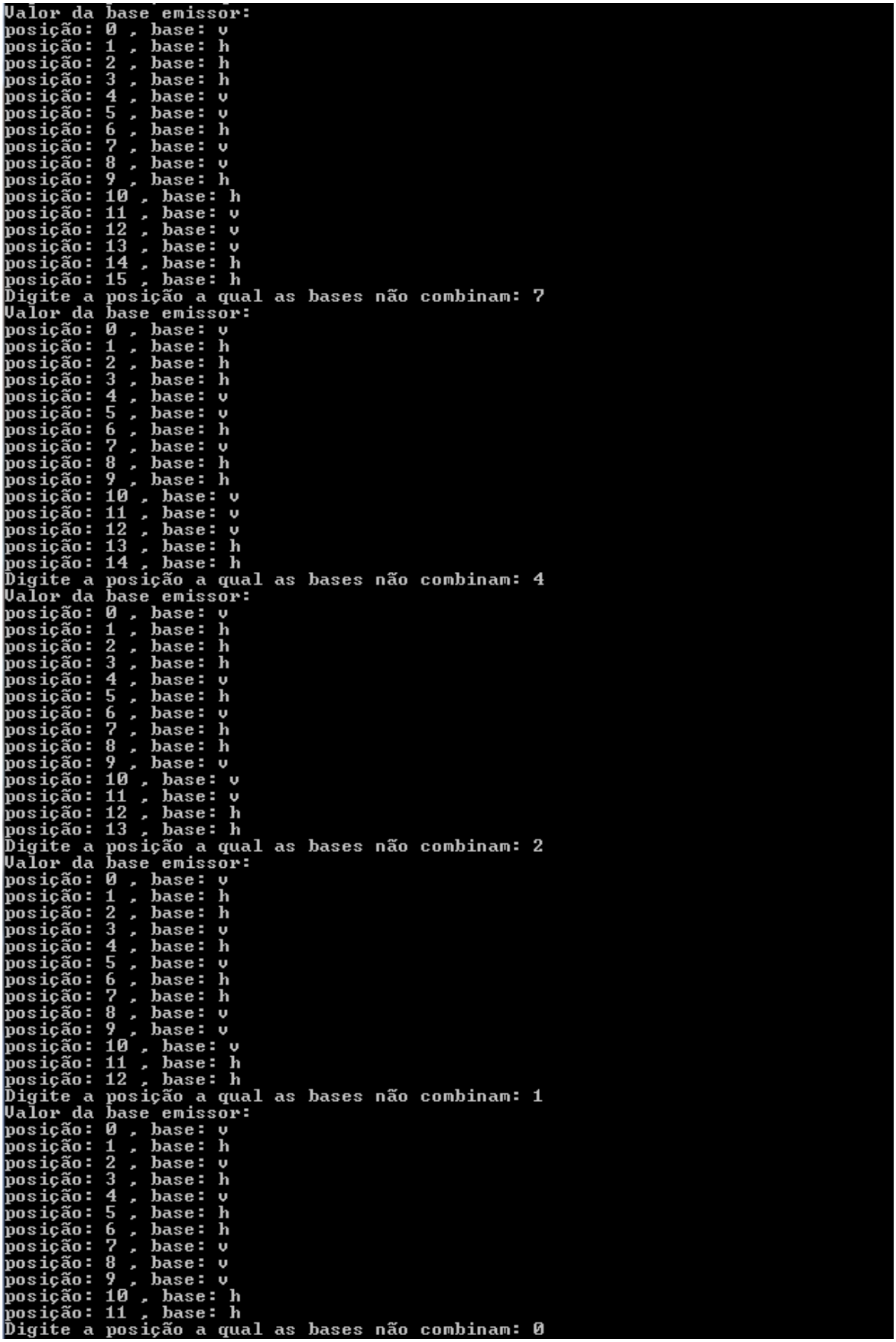
Fonte: Próprio autor (2020)

Figura 5 - Receptor retirando as bases da sequência parte 1.



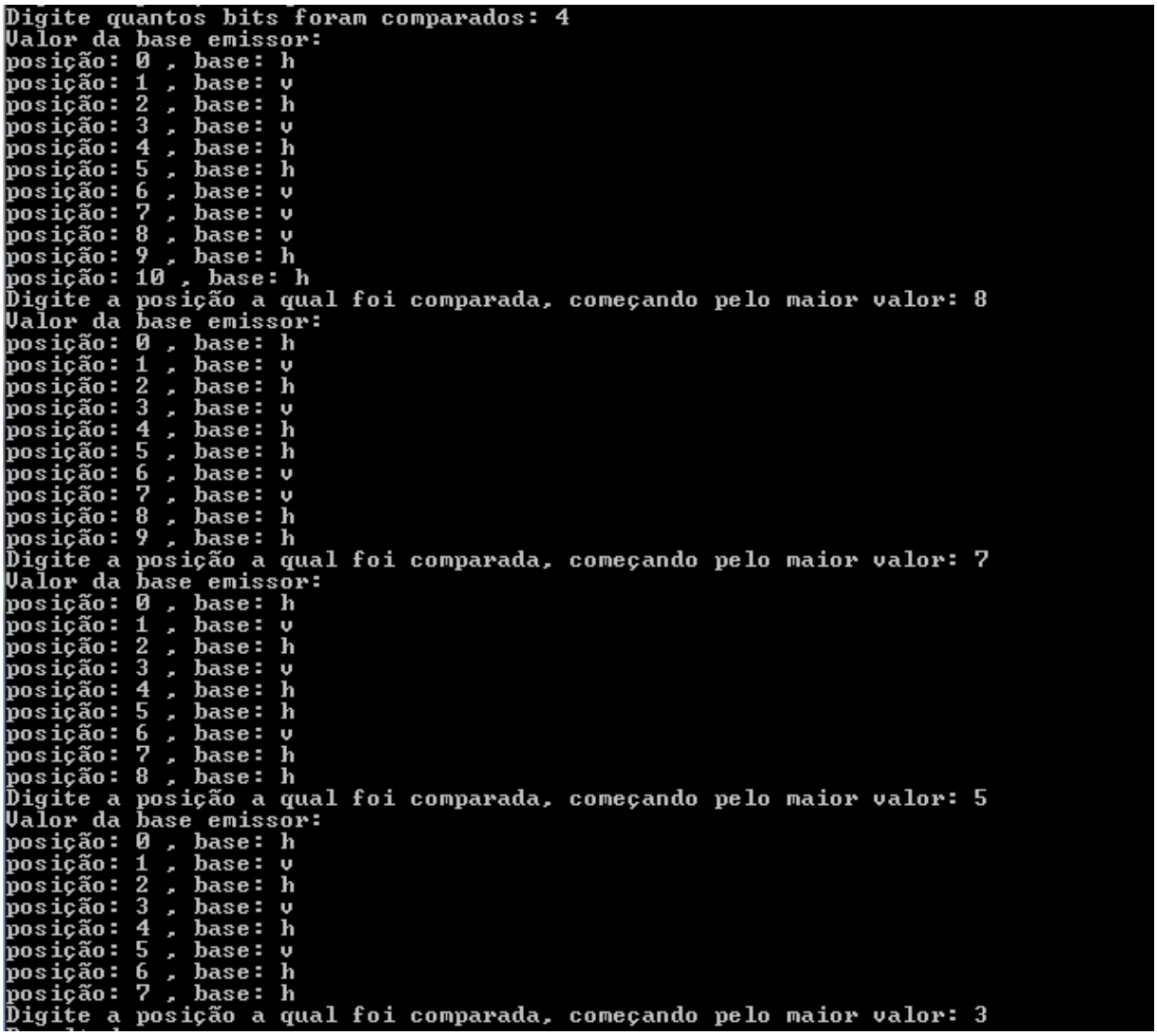
Fonte: Próprio autor (2020)

Figura 6 - Receptor retirando as bases da sequência parte 2.



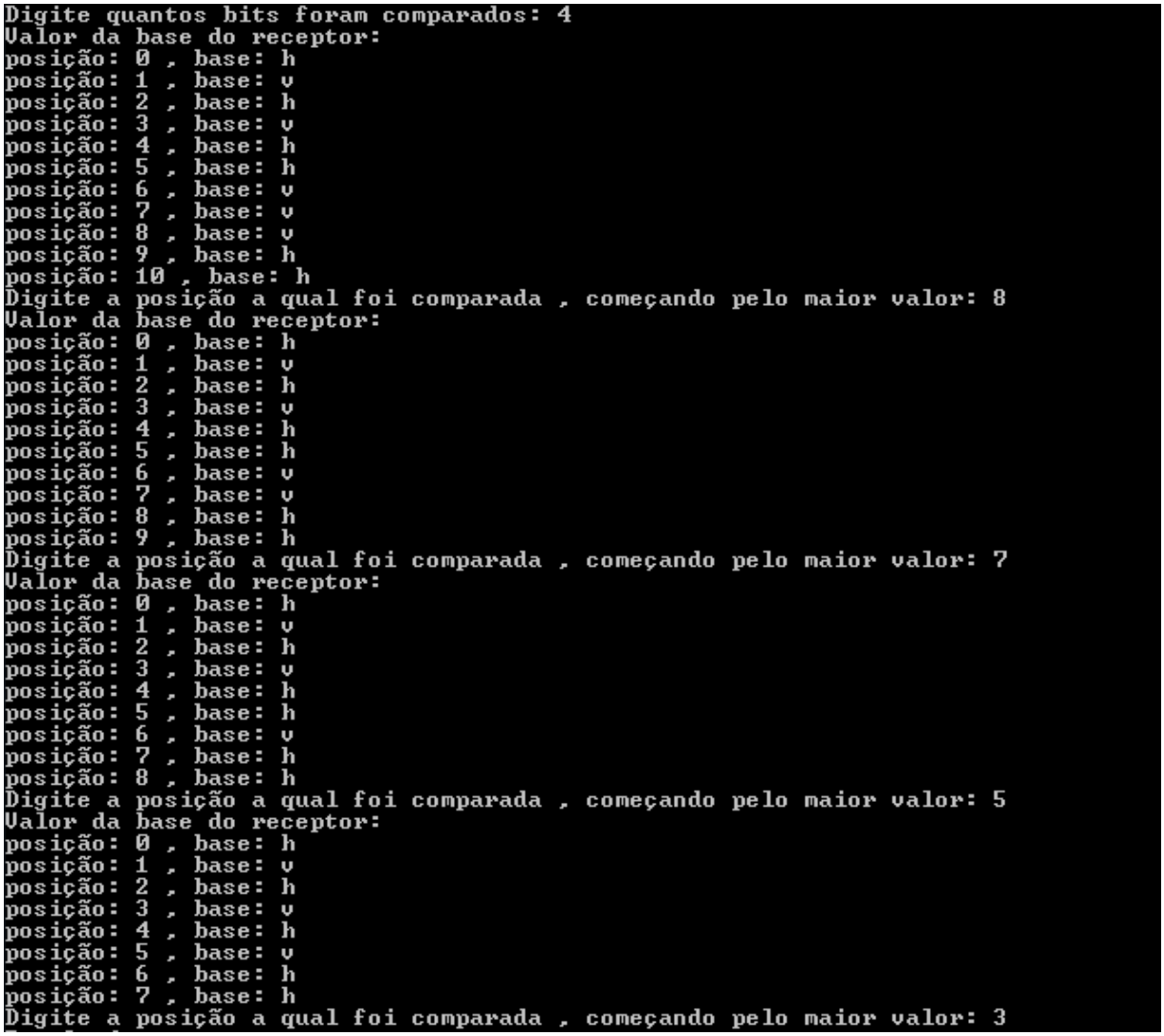
Fonte: Próprio autor (2020)

Figura 7 - Emissor retirando as posições.



Fonte: Próprio autor (2020)

Figura 8 - Receptor retirando as posições.

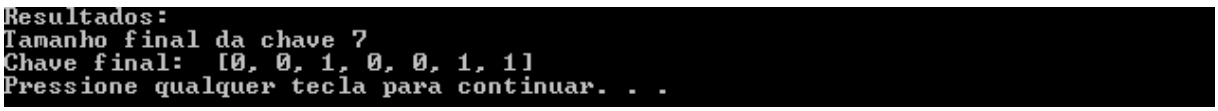


Fonte: Próprio autor (2020)

Figura 9 - Emissor recebendo o tamanho e valor da chave.

Fonte: Próprio autor (2020)

Figura 10 - Receptor recebendo o tamanho e valor da chave.



Fonte: Próprio autor (2020)