CAMPUS

CLAUDIO GABRIEL SANTOS PICININ – N076828 – Turma: SI2P68
GABRIEL DA COSTA NAKABAYASHI CAMPELO – N180EH2 – Turma: SI2P68
GUSTAVO HENRIQUE BAZOLLI ALVES – G87BGA4 – Turma: SI1P68
IZABELA HERMSDORF ANTONIASSI BASSANI – G802JJ4 – Turma: SI2P68
JOÃO VICTOR B. DA SILVA – G878JG6 – Turma: SI1P68
JOÃO VICTOR CAHUAYA MAYTA – F355FJ5 – Turma: SI1P68
KAYAN MAGALHÃES FILGUEIRA CHAVES – N0741G4 – Turma: SI2P68
LUAN DANTAS ARAUJO – R024547 – Turma: SI1P68
LUCAS FREITAS ABENANTE – G8388D5 – Turma: SI2Q68
RICARDO ALEXANDRE DE JESUS – N099755 – Turma SI2Q68

ATIVIDADES PRÁTICAS SUPERVISIONADAS - (APS):

AS TÉCNICAS CRIPTOGRÁFICAS, CONCEITOS, USOS E APLICAÇÕES

SÃO PAULO
2023/2

CLAUDIO GABRIEL SANTOS PICININ – N076828 – Turma: SI2P68
GABRIEL DA COSTA NAKABAYASHI CAMPELO – N180EH2 – Turma: SI2P68
GUSTAVO HENRIQUE BAZOLLI ALVES – G87BGA4 – Turma: SI1P68
IZABELA HERMSDORF ANTONIASSI BASSANI – G802JJ4 – Turma: SI2P68
JOÃO VICTOR B. DA SILVA – G878JG6 – Turma: SI1P68
JOÃO VICTOR CAHUAYA MAYTA – F355FJ5 – Turma: SI1P68
KAYAN MAGALHÃES FILGUEIRA CHAVES – N0741G4 – Turma: SI2P68
LUAN DANTAS ARAUJO – R024547 – Turma: SI1P68
LUCAS FREITAS ABENANTE – G8388D5 – Turma: SI2Q68
RICARDO ALEXANDRE DE JESUS – N099755 – Turma SI2Q68

ATIVIDADES PRÁTICAS SUPERVISIONADAS - (APS):

AS TÉCNICAS CRIPTOGRÁFICAS, CONCEITOS, USOS E APLICAÇÕES

Atividades Práticas Supervisionadas (APS), para o curso de Sistemas de Informação, apresentado para a Universidade Paulista – UNIP.

SÃO PAULO
2023/2

SUMÁRIO

1. Objetivo do Trabalho

A Atividade Prática Supervisionada tem como objetivo possibilitar que os alunos coloquem em prática as teorias aprendidas no decorrer do semestre nas disciplinas cursadas em sala de aula. Assim, o aluno terá oportunidade de praticar e estará mais próximo da realidade do mercado de trabalho. Assim, a APS deste semestre apresentou o cenário:

Um navio foi aprendido pela guarda costeira brasileira por transportar lixo tóxico da Ásia para a região norte do Brasil. O acesso à tripulação, assim como a todo conteúdo tóxico radiativo, deverá ser controlado. Somente inspetores devidamente trajados com roupas especiais poderão adentrar no navio. Por razões legislativas o navio deve permanecer a uma distância segura: 50 quilômetros da costa e todo e qualquer contato deverá ser realizado por meio de helicópteros, para minimizar e restringir o contato. A área do entorno num raio de 10 quilômetros está isolada.

A fim de praticar os ensinamentos de sala de aula, nos foi apresentado o desafio de desenvolver um programa em linguagem python que efetue a criptografia, descriptografia de qualquer mensagem, cifrada ou não, baseada na técnica escolhida pelo grupo, tratando-se de um espaço que envolve restrição de acesso a uma área contaminada com riscos à saúde pública.

2. Introdução

Este trabalho abordará a criptografia em suas várias formas e aplicações, explorando os princípios subjacentes, os métodos de implementação e os desafios emergentes enfrentados por aqueles que buscam proteger informações confidenciais em um mundo conectado. Além disso, examinaremos como a criptografia desempenha um papel fundamental na segurança cibernética, na proteção de dados corporativos e no avanço da pesquisa científica.

Neste trabalho o grupo mostra a relevância e a importância de utilizar a criptografia para a proteção de dados e arquivos, é muito comum vermos “vazamento de dados” de diversas empresas e até mesmo de diversas pessoas, vindo diretamente do uso da internet, visando que os casos de vazamento de informações confidenciais estão ocorrendo com mais frequência, uma das soluções que deve ser colocada em

prática é a criptografia. A grande necessidade está na proteção dos dados e identidade do próprio usuário, caso haja alguma invasão na tentativa de coletar dados do usuário, coletar arquivos confidenciais, se há a criptografia em seus sistemas ela fará a proteção de todos esses dados confidenciais, evitando assim que possa ocorrer o pior, com vazamento de diversos dados, arquivos, mensagens trocadas entre outras informações confidenciais, ela protege todas essas informações importantes. A utilização desta em cenários corporativos é de extrema importância como uma forma de segurança. Porém a criptografia não é só vantajosa nos meios corporativos, em ambientes domésticos também tem sua devida importância. O motivo é de sempre estarmos conectados com a internet, procurando, compartilhando e salvando informações online, sendo assim nossos dados estão sendo armazenados em algum local, onde muitas vezes não é 100% seguro, trazendo essa desconfiança para o usuário. Portanto a proteção com criptografia e aumento de segurança e privacidade em uso doméstico é de tamanha importância.

Os principais motivos que tornam necessária a utilização da criptografia são: proteger dados armazenados na nuvem, proteger informações de e-mail, proteger arquivos de acesso indevido, proteger dados de navegação, organizações a proteger os escritórios, proteger a propriedade intelectual, entre outros diversos motivos.

No trabalho apresentado iremos orientar como podemos realizar a criptografia tanto em redes corporativas quanto em redes domésticas, visto que há diversos tipos de criptografia que serão mencionados no decorrer do projeto. Além disso, o grupo mostra alguns conceitos utilizados nesse mundo da criptografia que poucos sabem, desde o início da criptografia, onde esse tema se encaixa no nosso dia a dia, os diferentes tipos de criptografia, além de apresentar diversas técnicas de utilizá-la, com o intuito de mostrar a importância do uso desta nos dias atuais. Porém o termo criptografia é muito antigo, diversas técnicas de ocultar mensagens foram utilizadas pelos gregos e romanos, com a necessidade do homem em guardar ou até esconder informações confidenciais desde sempre. Foi então desenvolvida diversas técnicas para ocultar mensagens, a criptografia pré-computacional foi formada por métodos de substituição e transposição de caracteres de uma mensagem que pudesse ser executada tanto manualmente como em alguns casos mentalmente, pelo emissor e pelo destinatário da mensagem.

A criptografia possui 4 objetivos principais como:

Confidenciabilidade: onde só o destinatário autorizado possui a capacidades de decifrar o conteúdo da mensagem;

Integridade: onde o destinatário deverá possuir a capacidade em vértices se a mensagem foi alterada ou não durante a transmissão;

Autenticação: o destinatário deverá verificar o remetente, se realmente ele é quem diz ser;

Irretratabilidade: não deverá ser possível ao remetente negar a autoria da mensagem.

Sendo assim, através de dois fatores podemos dizer que a criptografia é considerada segura computacionalmente, quando o custo para quebrar a criptografia excede o valor da informação criptografada, tornando-se bem-sucedida pois cada informação criptografada possui um determinado valor tanto para quem já possui, quanto para quem irá possuí-la. E ao tempo, quando ela acaba excedendo o tempo de vida útil da informação, e também quanto mais você investir o seu tempo para quebrar a criptografia, também significa que ela foi bem-sucedida.

No trabalho apresentado estará presente todas estas principais informações, além de conteúdos mais detalhados, então será possível aprender a criptografia desde sua existência, sua evolução, a importância do uso, como podemos utilizá-la, as técnicas dela, e diversas curiosidades apresentadas ao longo do trabalho.

3. Criptografia

A criptografia funciona através de algoritmos matemáticos que transformam dados legíveis em dados ilegíveis, conhecidos como *ciphertext*. Esses algoritmos são projetados de forma que apenas a pessoa com a chave correta possa decifrar o *ciphertext* e obter os dados originais, conhecidos como *plaintext*.

A criptografia desempenha um papel fundamental na segurança da informação em um mundo cada vez mais digital e interconectado. Ela é uma tecnologia que permite proteger dados sensíveis, tornando-os não acessíveis para qualquer pessoa que não tenha as chaves de descriptografia apropriadas. Nesta página, exploraremos a relevância da criptografia em diversos contextos. Como por exemplo:

Privacidade Pessoal: No ambiente digital atual, as informações pessoais são frequentemente compartilhadas e armazenadas online. Desde informações financeiras até mensagens pessoais, a criptografia ajuda a proteger a privacidade pessoal;

Segurança Empresarial: Empresas, independentemente de seu tamanho, lidam com uma quantidade significativa de dados sensíveis. A criptografia é essencial para proteger informações comerciais, como planos estratégicos, dados financeiros e informações do cliente;

Proteção de Transações Financeiras: Ela garante que as informações de pagamento e as transações sejam protegidas contra fraudes e acessos não autorizados;

Proteção de Dados em Trânsito: A criptografia de dados em trânsito garante que informações sejam protegidas enquanto são transmitidas de um ponto a outro, reduzindo os riscos de espionagem e interceptação;

Conformidade Legal: Em muitos países, existem regulamentações rigorosas relacionadas à proteção de dados pessoais e confidenciais. A criptografia ajuda as organizações a cumprirem essas regulamentações, garantindo a segurança dos dados dos clientes e funcionários;

Defesa Cibernética: A criptografia é uma camada fundamental de defesa contra-ataques cibernéticos, pois dificulta a extração de informações críticas, como senhas e dados financeiros.

A criptografia desempenha um papel crucial na proteção de dados sensíveis e na segurança da informação. Dois dos principais tipos de criptografia usados para essa finalidade são a criptografia simétrica e a criptografia assimétrica. Nas próximas páginas, vamos explorar esses dois métodos de criptografia, suas características e aplicações.

3.1. Criptografia simétrica e assimétrica

3.1.1 Criptografia simétrica

A criptografia simétrica é um dos métodos mais antigos e amplamente utilizados para proteger informações. Ela se baseia na ideia de que a mesma chave é usada tanto para criptografar quanto para descriptografar os dados. Aqui estão algumas características-chave:

- Chave Compartilhada: Ambas as partes envolvidas na comunicação devem possuir a mesma chave para criptografar e descriptografar os dados;
- Velocidade e Eficiência: A criptografia simétrica é notavelmente rápida e eficiente, tornando-a ideal para a criptografia de grandes volumes de dados;
  Exemplos de Algoritmos: Algoritmos como o AES (*Advanced Encryption Standard*) e o DES (*Data Encryption Standard*) são comuns na criptografia simétrica;
- Aplicações: A criptografia simétrica é frequentemente usada para proteger a confidencialidade de comunicações em tempo real, como chamadas de voz e videoconferências, além de garantir a segurança de arquivos armazenados em discos rígidos e mídias de armazenamento.

3.1.2 Criptografia asssimétrica

A criptografia assimétrica, também conhecida como criptografia de chave pública, é um método mais complexo e seguro em comparação com a criptografia simétrica. A principal diferença reside na utilização de um par de chaves: uma chave pública e uma chave privada. Eis algumas características importantes:

- Chave Pública e Chave Privada: Cada usuário tem um par de chaves: uma chave pública, que é compartilhada com todos, e uma chave privada, que é mantida em segredo;
- Mecanismo de Encriptação e Assinatura Digital: A chave pública é usada para criptografar mensagens e verificar assinaturas digitais, enquanto a chave privada é usada para descriptografar e assinar digitalmente mensagens;
- Segurança: A criptografia assimétrica é considerada mais segura do que a simétrica, pois não requer a troca de chaves secretas;
  Exemplos de Algoritmos: Algoritmos comuns incluem o RSA (Rivest-Shamir-Adleman) e o ECC (Elliptic Curve Cryptography);
- Aplicações: A criptografia assimétrica é amplamente usada em comunicações seguras pela internet, incluindo a autenticação de websites (usando SSL/TLS), e também desempenha um papel fundamental na autenticação de e-mails e assinaturas digitais.

Ambos os tipos de criptografia têm seu lugar no mundo da segurança da informação, e muitas vezes são usados em conjunto para atender as diferentes necessidades de segurança. A criptografia simétrica é eficiente e rápida, ideal para proteger grandes volumes de dados, enquanto a criptografia assimétrica fornece um nível mais elevado de segurança, especialmente em ambientes de comunicação pela internet, onde a confiança mútua é difícil de estabelecer. A escolha entre esses métodos depende dos requisitos específicos de segurança e das aplicações em questão.

A criptografia é essencial para garantir a segurança e a integridade dos dados em um mundo digital. Ela é uma ferramenta indispensável para a proteção da privacidade pessoal, a segurança empresarial e a conformidade legal, além de desempenhar um papel crucial na defesa contra ameaças cibernéticas. A importância da criptografia só tende a aumentar à medida que a nossa dependência da tecnologia digital cresce.

4. Técnicas criptográficas

4.1 Técnicas de criptografias mais utilizadas

Vamos falar sobre as técnicas de criptografia mais utilizadas. Existem muitas técnicas diferentes de criptografia, cada uma com suas próprias vantagens e desvantagens. Alguns exemplos incluem a criptografia simétrica, a criptografia assimétrica. Segundo NETSCAPE, as principais técnicas de criptografia são:

4.1.1. Criptografia simétrica

Na criptografia simétrica, a mesma chave é utilizada para encriptar e decriptar uma mensagem. Somente o remetente e o destinatário devem conhecer a chave secreta, pois esta é a única maneira de obter a confidencialidade.

O processamento necessário para a encriptação e decriptação é menor quando comparado ao da criptografia assimétrica. Com o um algoritmo força bruta é computacionalmente inviável, no caso médio, quebrar uma chave de 128 bits.

O maior problema dos algoritmos de criptografia simétrica é a distribuição da chave secreta, que precisa ser transmitida através de um canal de comunicação inseguro.

Os principais algoritmos de criptografia simétrica são DES (Data Encryption Standard), 3DES (Triple DES), IDEA (International Data Encryption Algorithm), RC2 e RC4 e AES (Advanced Encryption Standard).

4.1.2. Criptografia assimétrica

Na criptografia assimétrica, cada parte da comunicação possui um par de chaves. Uma chave é utilizada para encriptar e a outra para decriptar uma mensagem. A chave utilizada para encriptar a mensagem é publica, isto é, ela é divulgada para o transmissor; enquanto a chave para decriptar a mensagem é privada, isto é, ela é um segredo pertencente ao receptor. Sendo assim, não existe o problema de manutenção do segredo que existia na criptografia simétrica.

Os algoritmos de chave pública se caracterizam pelo uso de funções com elevada complexidade computacional. Utilizando um algoritmo força bruta é computacionalmente inviável, no caso médio, quebrar uma chave de 1024 bits. Os principais algoritmos de criptografia assimétrica são RSA, Diffie-Helman, DAS e Fortezza, sendo este último não suportado pelo TLS.

4.1.3. AES

O AES (Advanced Encryption Standard) é um algoritmo de criptografia simétrica que é amplamente utilizado para proteger dados confidenciais. Ele é considerado um dos algoritmos mais seguros disponíveis atualmente. O AES utiliza uma chave de criptografia para codificar e decodificar os dados, garantindo que somente pessoas autorizadas possam acessá-los. O AES é utilizado em diversos sistemas e aplicativos, incluindo sistemas operacionais, bancos de dados, aplicativos de mensagens e outros tipos de software que requerem segurança de dados.

5. Protocolos

Falando de protocolos, são conjuntos de regras que governam a comunicação entre dois dispositivos ou sistemas. Eles são usados para garantir que os dados sejam transmitidos com segurança e eficiência. Existem vários protocolos diferentes usados na comunicação digital, cada um com suas próprias características e finalidades

específicas. O SSL (Secure Sockets Layer) e o TLS (Transport Layer Security) são protocolos de segurança que visam proteger a comunicação entre um cliente e um servidor. Eles são usados para criptografar os dados transmitidos, garantindo que somente o destinatário possa lê-los. O SSL é a versão mais antiga desses protocolos, enquanto o TLS é a versão mais recente e segura. Segundo Microsoft temos então os protocolos:

5.1. SSL (Secure Sockets Layer)

SSL é um protocolo de segurança que permite a comunicação segura entre computadores na internet. Ele é utilizado para proteger informações transmitidas, como senhas e dados pessoais, contra interceptação e roubo por hackers. O SSL utiliza criptografia para proteger as informações transmitidas, garantindo que somente o destinatário correto possa acessá-las. O SSL é amplamente utilizado em transações financeiras, compras online e outras atividades que envolvem a troca de informações sensíveis pela internet.

5.2. TLS (Transport Layer Security)

O TLS (Transport Layer Security) é um protocolo de segurança amplamente utilizado, criado para aumentar a privacidade e a segurança dos dados em comunicações pela internet. Um dos principais casos de uso do TLS é a criptografia da comunicação entre aplicativos web e servidores, como quando um navegador carrega um site. O TLS criptografa a comunicação entre os computadores e o servidor de hospedagem no momento em que um site é acessado, garantindo que somente o destinatário possa lê-los. O TLS é a versão mais recente e segura do SSL (Secure Sockets Layer), que é a versão mais antiga desses protocolos.

Neste trabalho será explicado o protocolo TLS (Transport Layer Security) v1.1, visto que este é um padrão aberto e que é usado hoje na maioria das aplicações, com principal objetivo de fornece segurança em comunicações na Internet. O protocolo permite que aplicações cliente-servidor se comuniquem, garantindo a confidencialidade, a integridade e a autenticidade, ou seja segurança total, a alteração do conteúdo das mensagens e o envio de mensagens com remetente falso.

O principal objetivo do protocolo TLS é garantir a privacidade e a integridade dos dados em uma comunicação entre duas aplicações. O protocolo é composto de

duas camadas: o protocolo de Registro (TLS Record Protocol) e os protocolos Handshaking (TLS Handshaking Protocols).

O primeiro se localiza acima de um protocolo de transporte confiável (por ex: TCP), provendo a segurança da conexão que apresenta duas propriedades:

A conexão é privada. É utilizada criptografia simétrica para encriptação dos dados, por exemplo. As chaves para esta encriptação simétrica são geradas unicamente para cada conexão e são baseadas em um segredo negociado (ou negociação secreta) por um outro protocolo, neste caso o protocolo Handshake. O protocolo de Registro pode ser usado sem criptografia.

A conexão é confiável. O transporte da mensagem inclui uma verificação da integridade da mensagem, utilizando uma keyed-HMAC (Hashing Message Authentication Code). Funções hash seguras são utilizadas para computação da MAC. O protocolo de Registro pode operar sem uma MAC, porém geralmente, só é utilizado desta maneira, enquanto outro protocolo está usando o protocolo de Registro como transporte para a negociação dos parâmetros de segurança.

O protocolo de Registro é usado para a encapsulação de vários protocolos de níveis acima, por exemplo, o protocolo Handshake, que permite a autenticação entre cliente e servidor e a negociação de algoritmos de encriptação e de chaves criptográficas antes da transmissão ou recepção do primeiro octeto de dados por parte de um protocolo de aplicação. Os protocolos Handshaking provêem segurança da conexão que apresenta três propriedades:

A identificação de uma das partes pode ser autenticada através da criptografia assimétrica. Esta autenticação pode ser opcional, mas geralmente é exigida para pelo menos uma das partes.

A negociação de um segredo compartilhado é segura. O segredo negociado fica indisponível para terceiros, e para qualquer conexão autenticada o segredo não pode ser obtido, mesmo por um atacante que pode se colocar no meio da conexão.

A negociação é confiável. Nenhum atacante pode modificar a comunicação da negociação sem ser detectado pelas partes legítimas da comunicação.

Uma vantagem do TLS é a independência em relação aos protocolos de aplicação. Protocolos de nível acima podem comunicar com o TLS de forma transparente.

5.2.1. Objetivos

Os objetivos do protocolo TLS, em ordem de prioridade, são:

1°- Segurança com criptografia: TLS deve ser usado para estabelecer uma conexão segura entre duas partes.

2° - Interoperabilidade: Programadores independentes devem conseguir desenvolver aplicações utilizando TLS que possam trocar parâmetros criptográficos sem um conhecer o código do outro.

3° - Extensibilidade: TLS busca o fornecimento de uma estrutura (framework), em que novos métodos de criptografia simétrica e assimétrica podem ser adicionados, sem a necessidade da implementação de uma nova biblioteca de segurança.

4° - Eficiência Relativa: Operações de criptografia, principalmente de chave pública, exigem um alto processamento. Sendo assim, o protocolo TLS incorporou um mecanismo de armazenamento para evitar que toda conexão ao ser estabelecida não precise processar operações de criptografia. Com isso, reduz-se também a atividade da rede.

5.2.2. Protocolo de Registro

O TLS utiliza esta camada para encapsular todas as mensagens dos demais protocolos das camadas superiores, explicando a sua independência com os protocolos de aplicação, facilitando o desenvolvimento de aplicações que necessitam de conexões seguras. Enquanto os protocolos Handshaking realizam a negociação de parâmetros de segurança, o protocolo de Registro é quem realmente efetua as operações necessárias para garantir a segurança da conexão.

O protocolo de Registro recebe as mensagens para serem transmitidas, fragmenta os dados em blocos, opcionalmente realiza a compressão dos dados, aplica o MAC, encripta e transmite o resultado. Logicamente, com os dados recebidos, o protocolo de Registro realiza a decriptação, verificação da integridade, realiza descompressão, reagrupa os blocos e os entrega para as camadas superiores.

5.2.3. Protolocos de Handshaking

O TLS possui três sub-protocolos que permitem às partes chegarem a um acordo sobre os parâmetros de segurança que serão utilizados na camada de registro para autenticação, comunicação e para reportar condições de erro entre as partes.

O protocolo de Handshake é responsável pelos seguintes itens:

- Identificador da sessão: uma sequência de bytes escolhida pelo servidor para identificar uma sessão ativa ou uma sessão reiniciável.
- Método de compressão: qual o método de compressão que será utilizado antes da criptografia dos dados.
- Cipher Spec: especifica qual o algoritmo de criptografia vai ser utilizado, por exemplo, DES. Qual algoritmo de MAC (MD5, SHA) que vai ser utilizado. E define alguns atributos criptográficos como, por exemplo, o tamanho do hash.
- Chave Mestre (master key): chave secreta de 48 bytes que será compartilhada entre o cliente e o servidor.
- Is Resumable: flag que indica se a sessão pode ser utilizada para iniciar novas conexões.

Com os itens acima são criados os parâmetros de segurança para serem usados pela Camada de Registro para proteger os dados. Muitas conexões podem ser retomadas usando a mesma sessão, caso essa característica seja suportada pela mesma. Isso evita que todos os parâmetros de segurança tenham que ser novamente negociados.

5.2.4. Protocolo Change Cipher Spec

O protocolo Change Cipher Spec existe para sinalizar mudanças nas estratégias de criptografia que estavam sendo utilizadas. Este protocolo é formado por apenas uma mensagem, a qual é encriptada e comprimida com os parâmetros que estavam previamente estabelecidos.

A mensagem Change Cipher Spec é enviada por ambos, cliente e servidor, para que cada um deles passe a usar as novas regras de criptografia que foram negociadas.

Um cuidado deve ser tomado ao fazer as alterações nas estratégias de criptografia, pois existe a possibilidade de que o primeiro a receber a mensagem de

troca de estratégia possa ainda estar computando uma mensagem que recebeu anteriormente, já que os algoritmos de chave pública demandam muito processamento. Para resolver isso, deve ser esperado um tempo antes de mandar essa mensagem para garantir que o outro lado não perderá informações.

5.2.5. Protocolo de Alerta

Um dos tipos de conteúdo suportado pela camada de registros do TLS é o conteúdo de alerta.

As mensagens de alerta transportam a importância do alerta e a descrição do alerta. Mensagens com importância denominada fatal, resultam imediatamente no encerramento da conexão. Nesse caso outras conexões correspondendo à mesma sessão podem continuar, mas o identificador da sessão deve ser invalidado, prevenindo que essa sessão seja utilizada posteriormente para estabelecer novas conexões.

Assim como as outras mensagens do TLS, as mensagens de alerta também são encriptadas e comprimidas de acordo com os parâmetros de segurança que estão ativos no momento em que a mensagem é enviada.

Tipos de mensagem de alerta:

1° Alertas de Encerramento

São utilizados para informar às partes que a conexão será encerrada, evitando assim truncation attacks. Todos os dados recebidos após o recebimento de uma mensagem de encerramento são descartados.

2°Alertas de Erro

O tratamento de erros pelo TLS Handshake Protocol é muito simples. Quando um erro é detectado, quem detectou o erro envia um alerta para o outro lado. Se for um alerta fatal, imediatamente ambos terminam a conexão. Clientes e servidores devem esquecer quaisquer identificadores de sessões e chaves secretas associados com uma conexão que falhou. Por conseguinte, qualquer conexão que tenha sido encerrada por um alerta fatal não pode ser restabelecida. Exemplos de mensagem de erro são: bad_certificate, certificate_expired, illegal_parameter, unknown CA, insufficient security, entre outros.

3° Estabelecendo uma conexão

Os parâmetros criptográficos de uma sessão são determinados pelo TLS Handshake Protocol como já foi dito anteriormente. O TLS Handshake Protocol opera acima da camada de Registro.

Quando um cliente e um servidor começam a se comunicar eles têm que entrar em acordo sobre qual versão será utilizada, qual algoritmo criptográfico será usado, opcionalmente autenticar um ao outro e usar criptografia assimétrica para compartilhar um segredo a ser usado pela criptografia simétrica, que é responsável pela maior parte da criptografia realizada pelo protocolo.

O TLS Handshake Protocol é composto pelas seguintes etapas:

- Troca de mensagens de hello para chegar a um acordo sobre qual algoritmo criptográfico será usado, troca de valores aleatórios e checar se uma sessão está sendo restabelecida.
- Troca dos parâmetros criptográficos necessários para permitir ao cliente e ao servidor chegarem a uma premaster key.
- Troca de certificados para permitir que o cliente e o servidor se autentiquem.
- Gerar chave mestre (master key) a partir da premaster key.
- Informar a camada de registro sobre os parâmetros de segurança negociados.

Permitir que cliente e servidor possam verificar se ambos estão usando os mesmos parâmetros de segurança e verificar se a negociação não foi interceptada por um atacante.

O processo de negociação pode ser explicado da seguinte forma, o cliente envia uma mensagem de ClientHello para o servidor, o servidor deve então enviar de volta uma mensagem ServerHello, caso contrário um erro fatal será caracterizado e a conexão encerrada. As mensagens de Hello servem para estabelecer quais as capacidades de segurança cada um dos lados possui. Essas mensagens estabelecem os seguintes parâmetros: versão do protocolo, ID da sessão, Suíte de Criptografia e método de compressão. Adicionalmente dois valores aleatórios são gerados e trocados, ClientHello.random e ServerHello.random. Após a troca das

mensagens de Hello o servidor poderá enviar seu certificado, caso haja a necessidade de autenticação.

Alternativamente o servidor pode enviar uma mensagem de ServerKeyExchange se não possuir certificado ou se o seu certificado for utilizado apenas para assinatura digital. Se o servidor for autenticado, ele pode requisitar ao cliente um certificado, caso a suíte de criptografia requeira tal característica do cliente. Depois dessa fase o servidor envia uma mensagem de ServerHelloDone indicando que a fase de Hello da negociação acabou.

O servidor então passa a esperar que o cliente responda. Se o servidor pedir um certificado do cliente, então ele ficará esperando até que o cliente envie o certificado. O cliente então envia uma mensagem de ClientKeyExchange e o conteúdo dessa mensagem dependerá do algoritmo de chave pública escolhido na fase de Hello. Caso o cliente tenha enviado um certificado com capacidade de assinatura, uma mensagem de digitally-signed certificate verify será enviada para verificar o certificado. Nesse ponto a mensagem ChangeCipherSpec será enviada pelo cliente e este copiará para a mensagem as informações pendentes sobre as Cipher Specs. Logo após essa mensagem o cliente envia uma mensagem Finished, já utilizando todos os parâmetros de segurança negociados. Em resposta o servidor manda uma mensagem de ChangeCipherSpec e logo após uma mensagem de Finished já com os parâmetros de segurança negociado sendo utilizados para enviar a mensagem. Agora os dois lados já podem começar a transmissão dos dados de forma segura.

Para resumir uma sessão que já tem todos os parâmetros negociados, um processo mais simples é utilizado, o cliente envia uma mensagem ClientHello com o ID da sessão. O servidor então checa no seu cachê se possui os parâmetros daquela sessão. Se tiver e o servidor quiser resumir aquela sessão, então o servidor responde com uma mensagem ServerHello com o mesmo ID da sessão a ser resumida. Nesse momento ambos enviam uma mensagem de ChangeCipherSpec e procedem para o procedimento de encerramento do handshake com a mensagem Finished. Caso o servidor não encontre os parâmetros da sessão a ser resumida, todo o processo de handshake descrito acima terá de ser feito.

5.2.6. Análise de Segurança

O TLS só consegue estabelecer uma conexão segura se, no sistema do cliente e do servidor, as chaves e a aplicação forem seguras. Obviamente, a implementação do TLS deve estar livre de falhas de segurança.

O sistema é tão forte quanto mais forte for o mais fraco algoritmo de troca de chaves e autenticação suportado pelo TLS, e somente algoritmos de criptografia dignos de confiança devem ser usados. Chaves curtas só devem ser usadas se o valor do dado vale menos que o esforço necessário para decriptá-lo.

TLS suporta três modos de autenticação: autenticação de ambas as partes, somente o servidor autenticado ou anonimato total. Sempre que o servidor estiver autenticado, o canal está seguro contra - ataques, em que o atacante se posiciona entre o cliente e o servidor, logo sessões anônimas devem ser evitadas. Cada parte autenticada deve possuir um certificado válido, porém cabe a cada parte verificar tal validade e se ele não expirou ou se foi revogado.

TLS é suscetível a ataques de negação de serviço (DoS – Denial of Service). Em particular, um atacante que inicia um grande número de conexões pode causar um consumo de CPU do servidor, graças ao custo computacional de se utilizar criptografia.

6. Dissertação

Sabemos que o mundo tecnológico passou por diversas fases onde cada vez vivenciamos o impacto e os avanços que o mundo digital nos proporciona. Dentro desse nicho existem informações e dados que não podem cair em mãos erradas, ou serem divulgadas para qualquer pessoa. Dentro das empresas temos níveis hierárquicos que permitem restringir ou liberar informações sobre algo, a um certo grupo de pessoas; importante ressaltar que algumas empresas que dependem de um sistema, ou utilizam para fins específicos possuem pessoas de confiança para manusear e ditar quem poderá ver e acessar determinado arquivo. No entanto, ao subir um site, sistema bancário de pagamento, ou qualquer outra rede que necessite de segurança, estamos de certa forma, dando aos usuários mal intencionados, que se aproveitam de pequenas falhas de um sistema, a oportunidade de fazer o que bem entender com as informações obtidas. Sendo assim, tornou-se comum empresas

investirem cada vez mais em segurança cibernética, dentre essas medidas está a criptografia, para que não caiam em golpes ou sejam afetadas por hackers.

Engana-se quem acha que medidas de segurança para informações confidenciais surgiram somente com a tecnologia. De acordo com site, ramo estudantil IEEE, a palavra criptografia é de origem grega onde para sua formalização foram utilizadas outras duas palavras, sendo elas: “Kryptós” e “Gráphein”, que significam “oculto” e “escrever” respectivamente. Portanto, a palavra refere-se à maneira de se ocultar aquilo que fora escrito; a criptografia não impede a interceptação da mensagem, ela dificulta a compreensão de quem irá ler, sendo necessário saber a combinação que foi formatada para gerar o código escrito. Podemos dividir em duas partes a maneira como a criptografia esteve presente na humanidade, sendo eles o clássico e o moderno. O clássico, segundo o ramo estudantil IEEE, partem dos povos antigos do egito, mais especificamente conhecido a tumba de khnumhotep que trocava alguns hieróglifos, primeiro sistema de escrita do mundo e utilizados por volta de 3000 A.C de acordo com o ecycle, para que houvesse o aumento do mistério em torno da tumba. Outro marco importante, e muito conhecido é a “Cifra de César”, que foi utilizado pelo imperador Júlio César com a finalidade de proteger as mensagens que eram enviados para suas tropas em guerra, desta forma Júlio garantia a segurança que sua mensagem, mesmo se capturada, só seria decifrada por alguém que conhecesse e soubesse decifrar sua criptografia. A partir da modernização do mundo outros métodos de criptografia foram adotados e de diferentes formas no mundo, mas o que de fato marcou, e deu origem a modernidade, foi a criptografia utilizada na segunda guerra mundial, que não era muito diferente das anteriores porque mantinha o mesmo padrão de ocultar uma mensagem. Mas neste período tivemos a ajuda da tecnologia que ajudou ainda mais na propagação de mensagens codificadas para as tropas que estavam guerreando a quilômetros de distância.

O método de criptografia, através de um sistema atual, consiste em embaralhar e codificar dados legíveis para criar um ciphertext; um cipher converte um texto original em código não legível. O texto original é conhecido como código ilegível de ciphertext. No processo de transmissão de informação interna, o usuário envia os dados utilizando uma chave para codificar enquanto o usuário que recebe as informações utiliza a chave para decodificar os dados, mas a força ou potência de um sistema de criptografia depende do tamanho ou comprimento da chave utilizada, que

é medida em bits. Chaves que possuem um tamanho mais curto tendem a ter combinações menos seguras, pois será mais fácil conseguir decifrar a chave secreta.

Em contrapartida, chaves que são mais longas costumam ser mais seguras, apesar deste fato a criptografia consegue cumprir um papel fundamental na segurança de dados. Porém, para obtermos uma verdadeira fortaleza cibernética, é necessário aplicar outros métodos que ajudam a melhorar ainda mais a segurança de dados, sendo eles: Gerenciar o ciclo de vida da chave, que consiste na vida útil de uma criptografia onde para evitar que ela fique exposta a mau uso ou falhas de seguranças, deve gerar novas e eliminar os dados que não são mais úteis. Além disso, armazenar de forma protegida e segura seus dados pode ajudar na prevenção de problemas futuros com cibercriminosos, isso porque manter a chave criptografada em um módulo de segurança de hardware, HMS, ajuda a melhorar ainda mais a segurança da plataforma de armazenamento. Para um melhor entendimento, podemos utilizar como exemplo tecnológico a forma como os certificados SSL (secure Socker layer) funcionam. Eles habilitam a conexão HTTPS, que tem como objetivo realizar a segurança de transmissão de dados entre um navegador web e um visitante que acesse o servidor de hospedagem de um site.

De acordo com, MJV (Multinacional brasileira de transformação digital), existem 3 tipos de criptografias que se destacam e se tornam mais relevantes para segurança de dados de uma empresa, sendo elas; Funções Hash, chaves assimétricas e chaves simétricas onde podem ser subdivididas em frameworks; que são um conjunto de bibliotecas que abordam funcionalidades e estruturas para desenvolver aplicações. As funções hash são matemáticas, exatas e complexas pois os códigos alimentam os softwares do computador e são utilizados por eles para geração de novas chaves. A criptografia hash possibilita o cálculo de um identificador digital de tamanho fixo, conhecido como hash, a partir de textos de qualquer extensão, onde costumam ser compostos por 16 a 20 bytes, mas podendo se estender até 512 bytes.

Uma das principais características da função hash é sua eficiência no tráfego pois uma função deve ser completa, mas não pode ser pesada, logo, não poderá comprometer a velocidade de processamento e tráfego de dados. Além disso, a saída de tamanho é fixa, ou seja, o valor de entrada pode ser variável, mas as saídas devem sair no mesmo tamanho do código, isto é: possuem a mesma quantidade de letras, números e caracteres. A chave simétrica é o método mais simples e mais utilizado

devido a sua alta velocidade, no entanto apresenta um problema que pode acabar se tornando catastrófico porque emissor e receptor devem compartilhar a mesma chave e com isso acaba criando uma vulnerabilidade de segurança, e mesmo que seja relativamente pequena pode se tornar um problema maior no futuro. Por conta disso, as chaves simétricas, hoje em dia, não são mais recomendadas para o uso em informações de elevada importância.

As chaves assimétricas, que podem ser conhecidas por chave pública, possuem um par de chaves diferentes, sendo uma pública e a outra privada são usadas para codificar e decodificar informações, ou seja a chave pública realizar a criptografia e enquanto a chave privada a descriptografa. Quando alguém pretende realizar o envio de uma informação a outra de forma segura, a chave assimétrica usa a chave pública do destinatário para criptografar os dados e com isso o texto ou informação enviado se torna ilegível para qualquer pessoa que não possua a chave privada correspondente. Além disso, os dados são transmitidos pela rede e mesmo que interceptados por um cypher criminoso ela permanecerá ilegível caso ela não possua a outra chave para sua descodificação. E diferente da chave simétrica, a assimétrica permite que seja compartilhado abertamente uma chave pública, tirando assim a necessidade de uma outra chave secreta.

Diante do cenário e do tema proposto para formalização do projeto, o grupo realizou diversas pesquisas e em conjunto ficou acordado que para este caso aplicamos a utilização da criptografia simétrica em nosso trabalho. No cenário proposto para o grupo um navio que transportava lixo tóxico, vindo da Ásia, foi detido pela guarda costeira na região norte do Brasil e por conta disso o acesso a qualquer informação ou a seus tripulantes se tornou registro, logo deve ser criar uma rede de segurança em conjunto com setores responsáveis por este tipo de ocorrência, e para isso as informações devem ser passados e recebidas rapidamentes pelos os agentes encarregados na operação e para que isto ocorra de forma segura o uso da criptografia de dados torna se essencial neste cenário. De acordo com a Mailfence, a criptografia simétrica é, inicialmente, recomendada pois de acordo com a gravidade da situação as trocas de informações devem ser passadas rapidamente para as organizações responsáveis. Além disso, este tipo de codificação confidencial torna-se útil em casos onde o uso de recursos é menor, neste caso devido ao navio estar em alto mar, onde sua implantação é fácil, rápida e também não necessita de muitos recursos.

Outro ponto forte da simetria é o fato de, também de acordo com a mailfence, ela é ideal para lidar e transferir grandes quantidades de dados.No entanto, caso a operação esteja propensa a durar mais tempo ou seja descoberto algo que necessite maior confidencialidade o uso da linguagem simétrica pode não ser tão útil a longo prazo, pois se a chave for perdida os dados criptografados podem ser comprometidos e também algo que deve ser analisado é que esta chave deve ser compartilhada de forma segura para a outra parte, ou seja, o responsável pela criptografia deve enviar a forma como deve ser descriptografada a informação, portanto colocando assim em risco a integridade dos dados que devem ser mantidos em sigilo.

A medida com que os agentes passam a descobrir maiores informações sobre a companhia que estava transportava lixo para o norte brasileiro, é recomendável o uso da assimetria, pois em uma comparação com a simétrica, ela possui alguns pontos fortes que podem vir a serem mais seguros e efetivos durante as tratativas. de acordo com, mailfence, a assimetrica, diferentemente da anterior, só pode ser descriptografada com a chave privada do proprietário e caso seja perdida ou interceptada por pessoas má intencionadas, os dados não sofrem risco de serem comprometidos.

Mas é importante ressaltar que ela precisa de mais recursos e é mais lenta do que a anterior, ou seja, para que não haja problemas devem haver pontos de apoio, móveis ou fixos, próximos ao navio que forneçam todos os recursos necessários para que as informações transitem de forma segura. O grupo durante a elaboração para que obtivesse maior desempenho da codificação utilizou a codificação simétrica utilizando o método de + 7 caracteres, ou seja, casa letra escrita o sistema realizará a troca da letra aleatoriamente e em seguida, na próxima letra contará + 7 letras a frente e isso irá se repetir até o texto ou palavra ser totalmente criptografada.

Para realizar este projeto foi de extrema importância os ensinamentos obtidos tanto em sala de aula, como nas aulas online, onde podemos tirar maior proveito delas. Desta forma ao elaborarmos este projeto tivemos facilidade em desenvolver o assunto que nos foi proposto, A criptografia, e como ela seria utilizada em um cenário onde um navio é detido próximo ao norte brasileiro.

IPE - Introdução a programação estruturada - (conceitos basicos do python). Com as aulas de introdução a programação estruturada, aprendemos sobre os conceitos básicos da linguagem de Python, base que utilizamos para realização da criptografia.

LPA - Lógica de programação e algoritmos - Durante as aulas foi apresentado a base lógica para que pudéssemos realizar um programa de qualidade, graças a isso tivemos maior facilidade em elaborar o programa em python.

Lógica matemática - no trabalho a matemática foi essencial para criarmos a nossa criptografia, onde utilizamos algoritmos lógicos e matemáticos para realizar para que fosse gerada a criptografia

Comunicação e Expressão - Essa aula foi essencial para que pudéssemos elaborar e dissertar sobre o projeto, aplicarmos os conhecimentos obtidos. Teoria geral dos sistemas - Estas aulas foram cruciais para compreender e adquirir com maior facilidade um sistema como um todo.

Dessa forma, o grupo concluiu que a criptografia é uma ferramenta essencial e poderosa no atual cenário digital, além também de ter seu papel no passado onde desde a Cifra de César, utilizada por Júlio César na roma antiga já demonstraram a importância de ocultar as informações desde os tempos imemoriais. Ela exerce uma função fundamental na proteção à privacidade, na segurança de informações e na integridade de dados.

Com a evolução digital passaram a criar outras formas de criptografia bem como a simétrica e assimétrica. Onde ambas possuem diferenças em seu formato de utilização, mas que tem o mesmo objetivo.

Para o nosso projeto, pensamos em usar a criptografia simétrica, pois dentro do cenário marítimo na qual nos foi apresentado, pensamos na velocidade que este tipo de criptografia pode entregar, sendo ela, em uma breve comparação com a assimétrica, a mais rápida.

Portanto, em resumo a criptografia desempenha um enorme papel na segurança de informações confidenciais em um mundo cada vez mais avançado tecnologicamente. Historicamente a evolução da confidencialidade de informações demonstra a adaptação constante para que fossem atendidas as mudanças na qual o mundo sofreu, e sua aplicação neste projeto tem como propósito destacar a sua importância no cenário atual de segurança cibernética. Desta forma é crucial reconhecermos a relevância contínua da criptografia e investir em seu aprimoramento para que possamos enfrentar os desafios emergentes desta era tecnológica.

7. Projeto Estruturado

Para este semestre nos foi apresentado um novo desafio, onde cada grupo deveria criar um programa que realizasse a criptografia e descriptografia de um texto. Mas para isso deveríamos nos basear em um caso fictício, onde um navio estrangerio foi interceptado pela Marinha Brasileira transportando lixo tóxico. Após realizarmos pesquisas e análises, o grupo se reuniu para poder realizar a divisão de tarefas que cada membro deveria fazer e a partir deste encontro o projeto foi sendo desenvolvido.

O objetivo do projeto foi abordar de forma ampla os princípios básicos e mais complexos da criptografia no mundo antigo e nos tempos atuais. Sabemos que o ato de criptografia surgiu a muitos anos, mas, com o avanço dos recursos utilizados pela humanidade, sofreu diversas mudanças e adaptações importantes durante o avanço dos seres humanos. Em um passado não tão distante, especificamente na segunda guerra mundial a criptografia foi de extrema importância para que as tropas que estavam em conflitos pudessem se comunicar, e mesmo que os códigos fossem interceptados somente os detentores da chave que possuía a descodificação poderiam receber a mensagem. Em nosso projeto decidimos dar maior ênfase na criptografia que conhecemos atualmente e é que mais vemos ao longo do dia, por exemplo; Ao acessar qualquer rede social nós estamos sendo protegidos por códigos que tem como papel garantir que nenhuma informação pessoal seja exposta indevidamente ou que algum invasor tenha fácil acesso a este tipo de conteúdo, além disso o principal alvo dos hackers são cartões que cadastramos ao em sites online, por isso devemos nos atentar quando formos realizar compras online em sites não muitos conhecidos. Com o avanço da comunicação tecnológica não foram apenas as compras online que revolucionaram o mundo, a troca de informações entre empresa e organizações de importância mundial também se tornaram usuários fiéis da criptografia digital, isto porque com poucos cliques é possível enviar uma mensagem de um continente ao outro.

Para que pudéssemos desenvolver um programa que realizasse uma operação deste nível, foi necessário utilizar e aprender os conceitos básicos ensinados durante algumas aulas de IPE (introdução a programação estruturada), e também realizar pesquisas mais complexas para que houvesse êxito na entrega do que nos foi pedido. Diante do cenário que nos foi proposto, tivemos que nos reunir diversas vezes para discutirmos e analisarmos de forma cautela a situação em que o navio se encontrava

pois mesmo que fosse um simples programa de envio e recebimento de mensagem nós deveríamos elaborar algo que fosse fácil de ser compreendido, haja visto que o situação em que o navio se encontra era de extrema segurança porque o mesmo ainda encontrava se em alto mar e a todo instante era vigiado, além também de que os tripulantes não poderiam sair daquela embarcação até que tudo que o caso fosse encerrado. Somente o pessoal autorizado poderia acessar a embarcação e mesmo assim deveriam utilizar roupas com proteção radioativa. Desta forma o grupo decidiu que deveríamos criar algo que pudesse ser de fácil acesso aos responsáveis pela operação e também que não necessitasse de muitos recursos, pois o estava em alto mar. Sabendo disso o programa foi desenvolvimento usando a criptografia simétrica que tem como característica, em uma breve comparação com a assimétrica ela é mais rápida no processamento, a sua facilidade em implementar e usar é ideal para a transferência de dados em grandes quantidades. Em nosso programa colocamos o número de deslocamento, ou chave, para “+7” ou seja, caso o agente queira enviar a mensagem criptografada para alguém, o código irá contar mais 7 letras para frente da qual ele digitou, por exemplo: Caso a letra A seja selecionada, na criptografia aparecerá G. Assim o programa terá uma segurança maior durante a troca de mensagens, mas caso a sejam descobertas informações que exijam maior confidencialidade será necessário realizar um programa com o tipo assimétrico pois ele possui maior capacidade de proteção de dados, e é mais recomendável para situações mais sigilosas.

Neste projeto tivemos a oportunidade de utilizar a imaginação, de acordo com o cenário, para criarmos um programa que tivesse o objetivo de realizar a proteção de dados confidenciais sendo um grande desafio pois no mundo real existem pessoas que de fato trabalham com esse tipo de função. Eles devem ser capacitados e desenvolver programas que protegem informações de nível básico a nível de extrema confidência. Para nós que estamos iniciando a carreira na área de desenvolvedor ou programador, este tipo de projeto nos ajuda a entender melhor o mercado e conhecer nichos que dificilmente pesquisarmos a fundo. Logo este tipo de trabalho nos ajuda a melhor a base de conhecimentos e descobrir habilidades em determinadas funções

Portanto, o grupo concluiu que este projeto nos fez aprender mais sobre a criptografia e seus vários tipos de formatação, E também contribuiu para que pudéssemos analisar melhor a rotina que levamos diariamente, pois conforme mencionada a a codificação de dados está em todos os lugares em que existe internet,

desde do caixa eletrônico ao celular que mexemos todos os dias. Com estas informações agora enxergamos o mundo da tecnologia de outra forma, pois sabemos que existe uma enorme rede de pessoas que trabalham para tentar nos proteger de invasores mal intencionados.

8. Código

```
def criptografar(texto):
    resultado = ""
    for char in texto:
        if char.isalpha():
            shift = 7
            if char.islower():
                ascii_offset = ord('a')
            else:
                ascii_offset = ord('A')

            criptografado = chr((ord(char) - ascii_offset + shift) % 26 + ascii_offset)
            resultado += criptografado
        else:
            resultado += char
    return resultado

def descriptografar(texto):
    resultado = ""
    for char in texto:
        if char.isalpha():
            shift = 7
            if char.islower():
                ascii_offset = ord('a')
            else:
                ascii_offset = ord('A')
```

```
            descriptografado = chr((ord(char) - ascii_offset - shift) % 26 + ascii_offset)
            resultado += descriptografado
        else:
            resultado += char
    return resultado

texto_original = input("Digite o texto que você deseja criptografar: ")
texto_criptografado = criptografar(texto_original)

print("\nTexto criptografado:")
print(texto_criptografado)
print("\n--------------------------------\n")

while True:
    escolha = input("Escolha uma opção:\n1 - Descriptografar\n2 - Sair\n")

    if escolha == "1":
        print("\nTexto original:")
        print(texto_original)
        print("\n--------------------------------\n")
    elif escolha == "2":
        break
    else:
        print("Opção inválida. Por favor, escolha 1 ou 2.")
```

REFERÊNCIAS

ALENCAR FILHO, E. de. Iniciação à lógica matemática. São Paulo: Nobel, 2002.

CÍNTIA. B. Um Mecanismo Para Distribuição Segura de Vídeo MPEG. Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de Mestre em Engenharia.2000. pág. 23-55.

CRIPTOGRAFIA: origem e história. Disponível em: https://www.ieeeuel.org/post/criptografia-origem-e-hist%C3%B3ria. Acesso em: 01 out. 2023.

CRIPTOGRAFIA simétrica e assimétrica: Qual é a diferença? Disponével em: https://blog.mailfence.com/pt/criptografia-simetrica-x-assimetrica-qual-e-a-diferenca/#:~:text=A%20criptografia%20sim%C3%A9trica%20%C3%A9%20mais,n%C3%A3o%20quiser%20correr%20nenhum%20risco. Acesso em 16 out. 2023.

DAGLIAN, J., Lógica e Álgebra de Boole – 4ª. Ed. – São Paulo: Atlas, 1995.

D'OTTAVIANO, Í. M. L., FEITOSA, H. A., Sobre a história da lógica, a lógica clássica e o surgimento das lógicas não-clássicas. V SEMINÁRIO NACIONAL DE HISTÓRIA DA MATEMÁTICA. Rio Claro. Abr. de 2003. Disponível em: <ftp://ftp.cle.unicamp.br/pub/arquivos/educacional/ArtGT.pdf>. Acesso em: 22 set. 2023.

DEVMEDIA. Disponível em: https://www.devmedia.com.br/criptografia-conceito-e-aplicacoes-revista-easy-net-magazine-27/26761. Acesso em 15 out. 2023.

KANT, K., Iyer, R., Mohapatra, P. Architectural Impact of Secure Socket Layer on Internet Servers. Em Proc. Int. Conf. Computer Design, 2000. pág 7-9.

MAOR, E. A história de um número. Rio de Janeiro: Record, 2003.

MENEZES, A. J.; VAN OORSCHOT, P. C.; VANSTONE, S. A. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996. Disponível em: <http://cacr.uwaterloo.ca/hac/>. Acesso em: 10 out. 2023.

MENEZES, N. N. C. Introdução à Programação com Python: algoritmos e lógica de programação para iniciantes. São Paulo: Novatec, 2019.

MJV. Os 10 tipos de criptografia mais relevantes nos negócios. Disponível em: https://www.mjvinnovation.com/pt-br/blog/tipos-de-criptografia/. Acesso em: 09 set. 2023.

NETSCAPE. NETSCAPE. SSL 3.0 SPECIFICATION. Disponível em http://wp.netscape.com/eng/ssl3/. Acesso em 19 out. 2023.

RAMALHO, L. Python fluente: programação clara, concise e ficaz. São Paulo: Novatec, 2015.

SHACHAM, D., E BONEH, D. Improving SSL Handshake Performance via Batching. Em ed. D. Naccache, editor, Proceedings of RSA 2001, volume 2020 (Springer-Verlag, 2001), pág 1-2.

SUN. Introduction to SSL. Disponível em http://docs.sun.com/source/816-6156-10/contents.htm#1041986. Acesso em 20 out. 2023.

TAHAN, M. O homem que calculava. Rio de Janeiro: Record, 2001.

TANENBAUM. TANENBAUM, A., Computer Networks. Prentice Hall, 1996. pág 864-868RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1

TECHONLINE. SSL and TLS Essentials: Securing the Web. Disponível em http://www.techonline.com/community/tech_topic/internet/feature_article/14364. Acesso em 7 set. 2023.

ZELLE, J. M. Python Programming: an introduction to computer science. 3. ed. New York: Franklin, Beedle & Associates Inc, 2016.