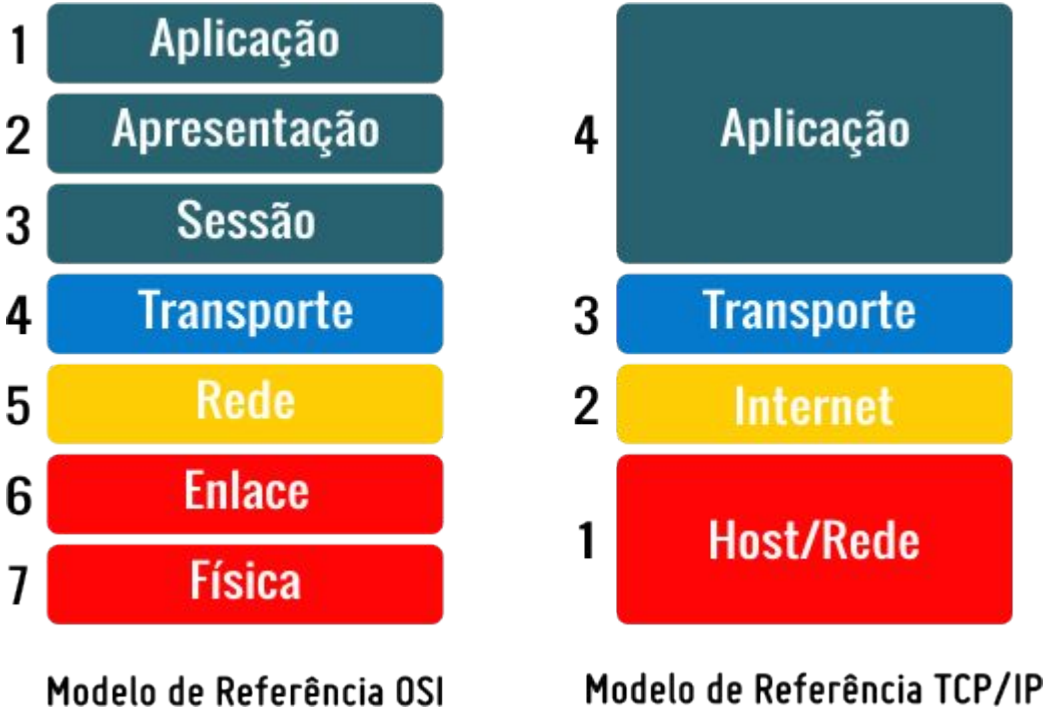
Recuperação - Redes

Slide completo

MODELO OSI x MODELO TCP/IP



MODELO TCP/IP

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAHIA

Existe um debate sobre a quantidade de camadas do modelo TCP/IP, sendo tratado em alguns materiais didáticos como um modelo de 5 camadas (ganhando a camada de enlace) e em outros por 4 camadas (modelo apresentado no slide anterior).
As duas formas podem ser encontradas na documentação de referência, mas para facilitar nossos estudos utilizaremos o modelo de 4 camadas.

CAMADA DE APLICAÇÃO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAHIA

A camada de aplicação, gerencia os protocolos de comunicação de nível mais alto, ou seja, aqueles como os quais o usuário possui contato direto, como é o caso do HTTP, DNS, FTP, POP, SMTP, entre outros.

Esta camada faz a comunicação entre os programas e os protocolos de transporte no TCP/IP, que será a próxima camada.

CAMADA DE APLICAÇÃO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAHIA

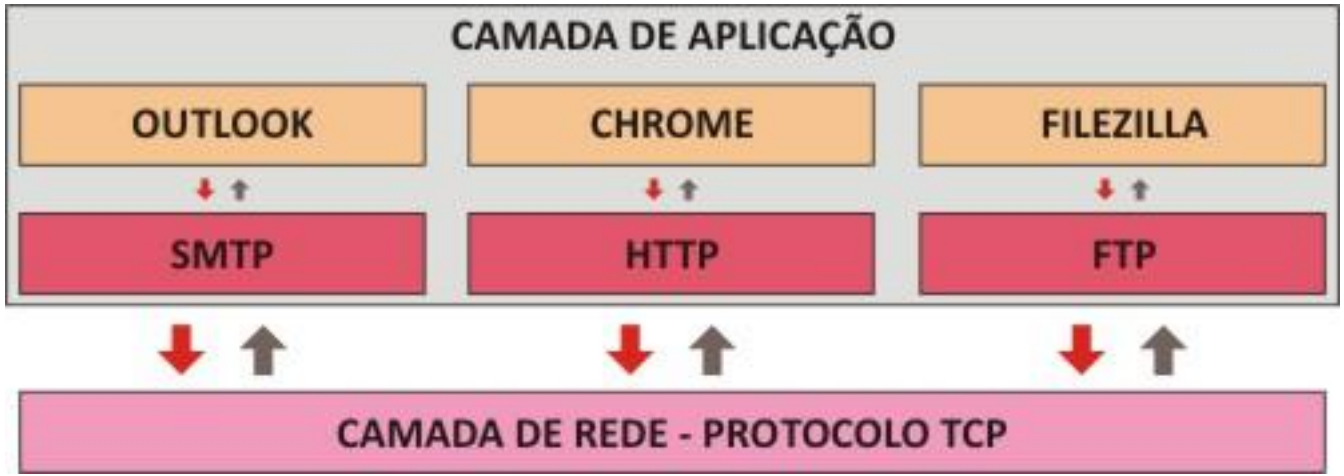
Protocolos que estudaremos da camada de aplicação:

- O HTTP é utilizado para a comunicação de dados da internet – WWW;
- O FTP é utilizado para a transferência de arquivos de modo interativo;
- O DNS é utilizado para resolver o nome de um host em endereço IP;
- O DHCP é utilizado para oferecer dinamicamente endereços de rede.
- O TELNET é utilizado para proporcionar uma facilidade de comunicação baseada em texto interativo bidirecional usando uma conexão de terminal virtual.

CAMADA DE APLICAÇÃO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAHIA

As aplicações geram dados em sua forma básica.



CAMADA DE TRANSPORTE

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAHIA

Esta camada é responsável por receber os dados enviados pela camada de aplicação e transformá-los em pacotes menores, a serem repassados para a camada de internet. Ela garante que os dados chegarão sem erros e na sequência correta.

É formado por dois protocolos, o TCP e UDP.

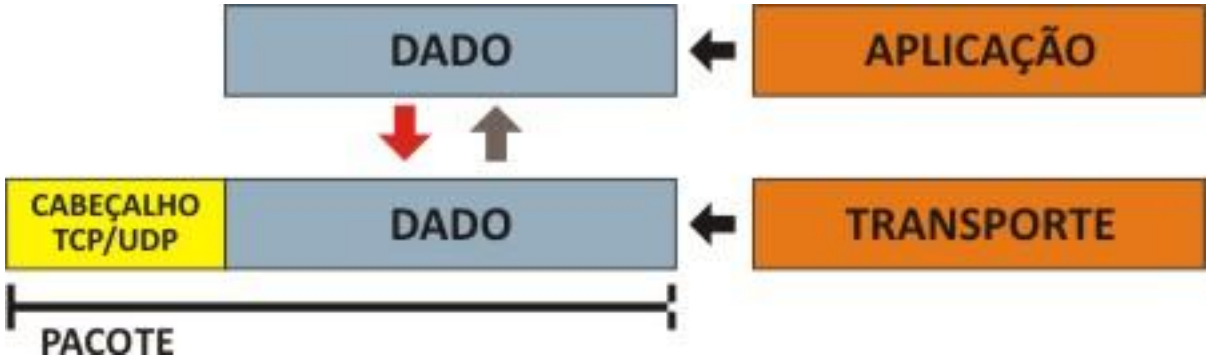
CAMADA DE TRANSPORTE

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAHIA

- O protocolo UDP realiza apenas a multiplexação para que várias aplicações possam acessar o sistema de comunicação de forma coerente. Não possui confirmação de entrega e é geralmente usado na transmissão de informações de controle.
- O protocolo TCP realiza, além da multiplexação, uma série de funções para tornar a comunicação entre origem e destino mais confiável. São responsabilidades do protocolo TCP: o controle de fluxo e erro, a sequência e a multiplexação de mensagens.

CAMADA DE TRANSPORTE

O dado criado através da aplicação passa a receber um cabeçalho.



CAMADA DE INTERNET

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAHIA

Ela é responsável pelo endereçamento e roteamento do pacote, fazendo a conexão entre as redes locais. Adiciona ao pacote o endereço IP de origem e o de destino, para que ele saiba qual o caminho deve percorrer.

Na transmissão, o pacote de dados recebido da camada de transporte é dividido em pedaços chamados datagramas. Os datagramas são enviados para a camada de interface com a rede (última camada), onde são transmitidos pelo cabeamento da rede através de quadros.

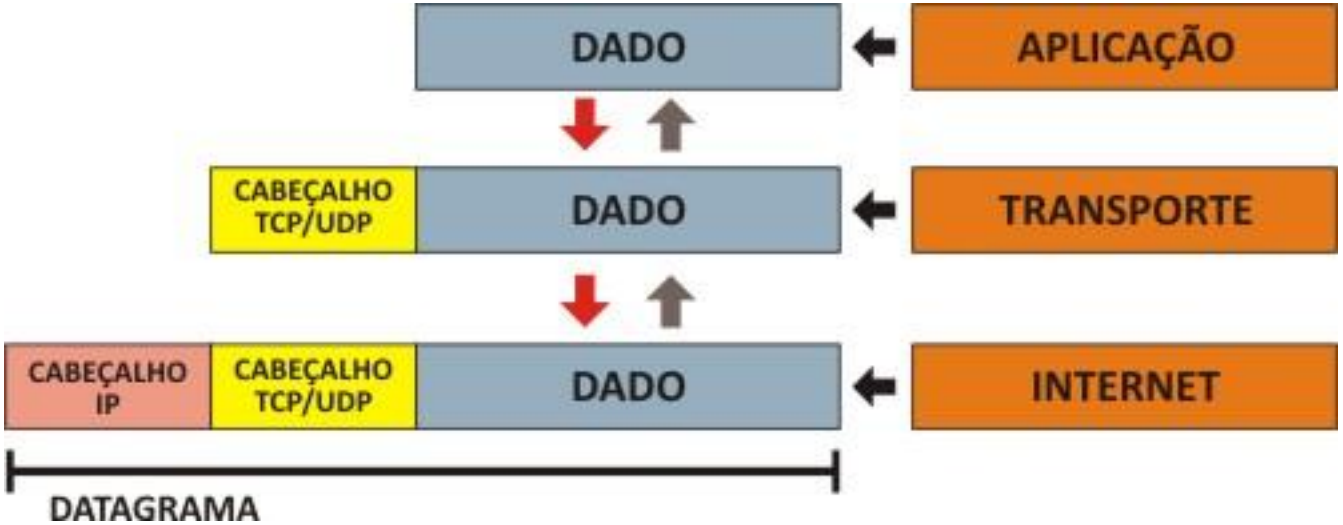
CAMADA DE INTERNET

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAHIA

Os protocolos principais da camada da Internet são IP, ARP, ICMP e IGMP.

- O IP é um protocolo roteável responsável pelo endereçamento IP, fragmentação e montagem dos pacotes;
- O ARP é responsável pela resolução do endereço da camada de internet para o endereço da camada de interface de rede, tais como um endereço de hardware;
- O ICMP é responsável por fornecer funções de diagnóstico e relatar erros devido à entrega bem sucedida de pacotes IP;
- O IGMP é responsável pela gestão dos grupos de multicast IP.

CAMADA DE INTERNET



CAMADA DE REDE

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAHIA

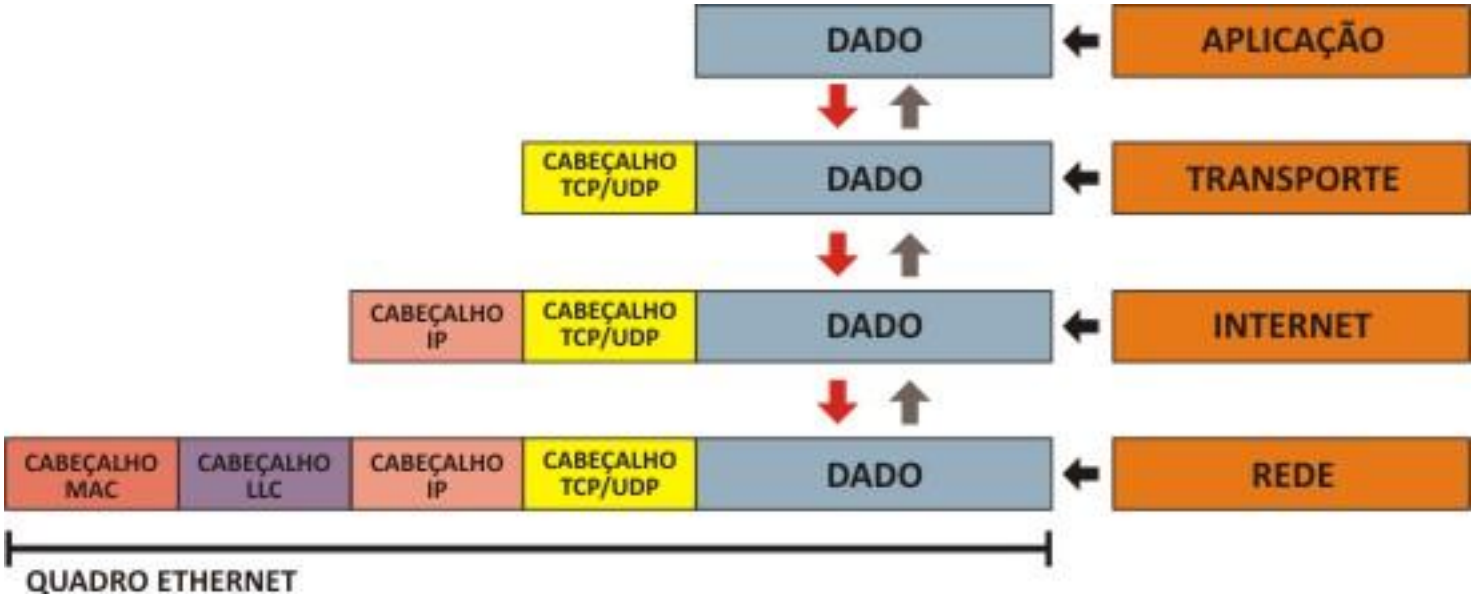
Essa camada é responsável pelo envio do datagrama recebido da camada de internet em forma de quadros através da rede física. Ela garante as seguintes noções: encaminhamento dos dados na conexão, coordenação da transmissão de dados (sincronização), formato dos dados, conversão dos sinais (analógico/numérico), controle dos erros na chegada, etc.

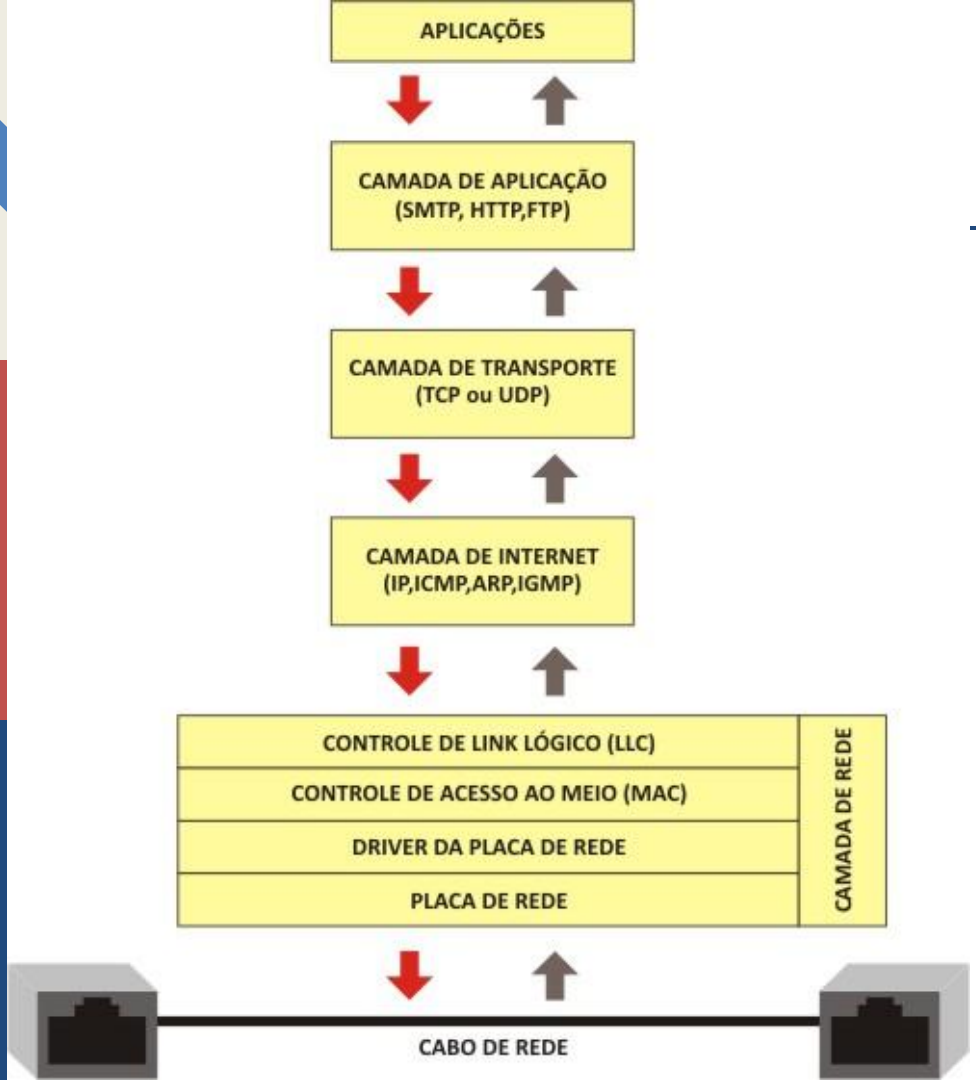
CAMADA DE REDE

O Ethernet é o protocolo mais utilizado e possui três componentes principais:

- Logic Link Control (LLC): responsável por adicionar ao pacote, qual protocolo da camada de internet vai entregar os dados para a serem transmitidos. Quando esta camada recebe um pacote, ela sabe para qual protocolo da camada de internet deve ser entregue.
- Media Access Control (MAC): responsável por montar o quadro que vai ser enviado pela rede e adiciona tanto o endereço origem MAC quanto o endereço destino, que é o endereço físico da placa de rede.
- Physical: responsável por converter o quadro gerado pela camada MAC em eletricidade (se for uma rede cabeada) ou em ondas eletromagnéticas (se for uma rede wireless).

CAMADA DE REDE



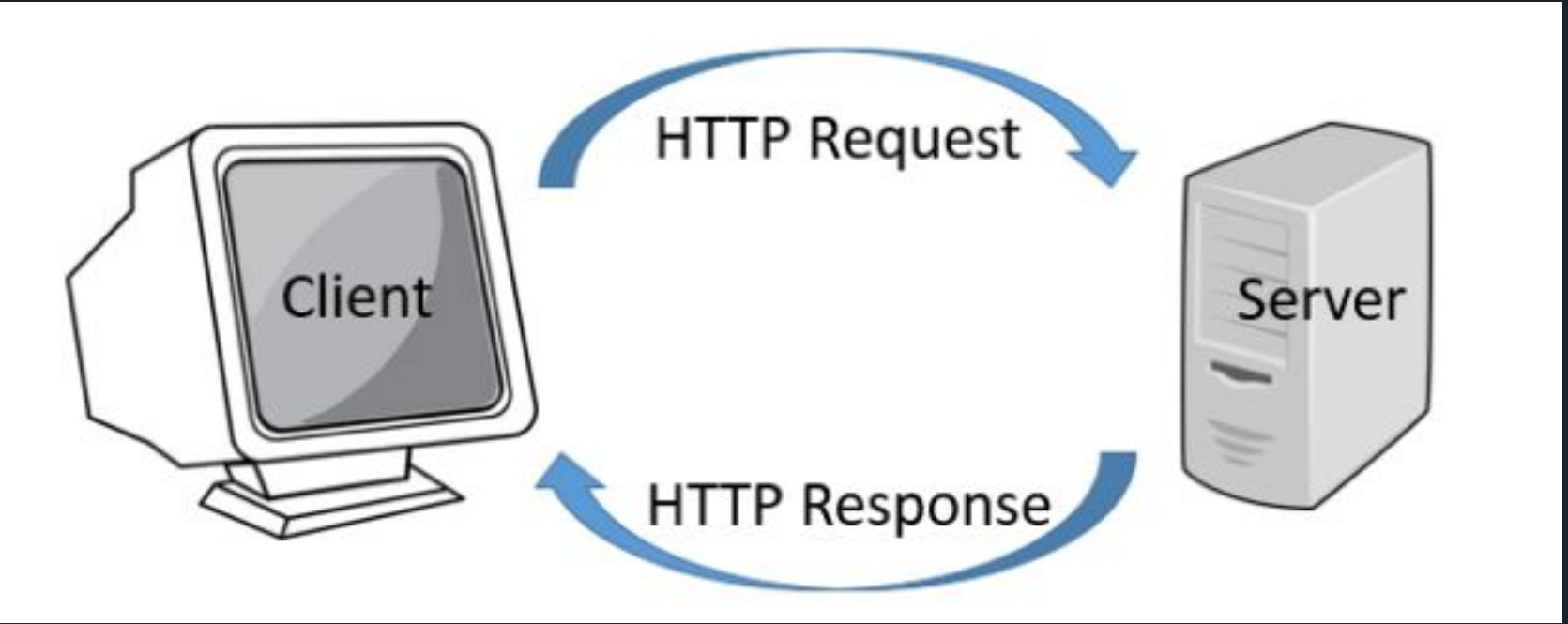


INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
BAHIA

Esse é o caminho que um dado realiza no seu tráfego pela rede, iniciando na aplicação de um usuário e terminando em uma outra aplicação. Esse ciclo é chamado de *encapsulamento*

Protocolo HTTP

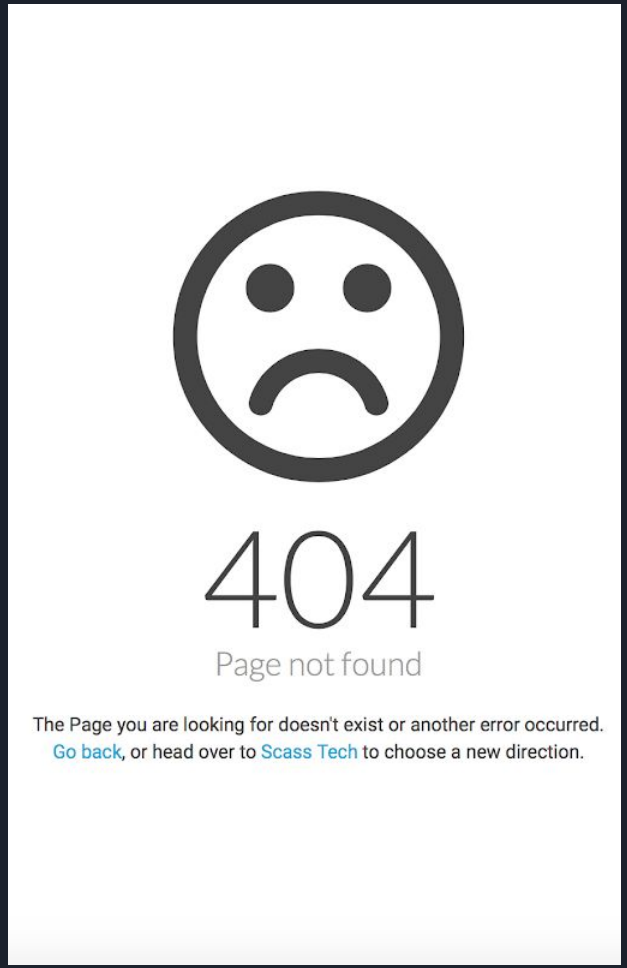
Cliente vs Servidor



Request e Response

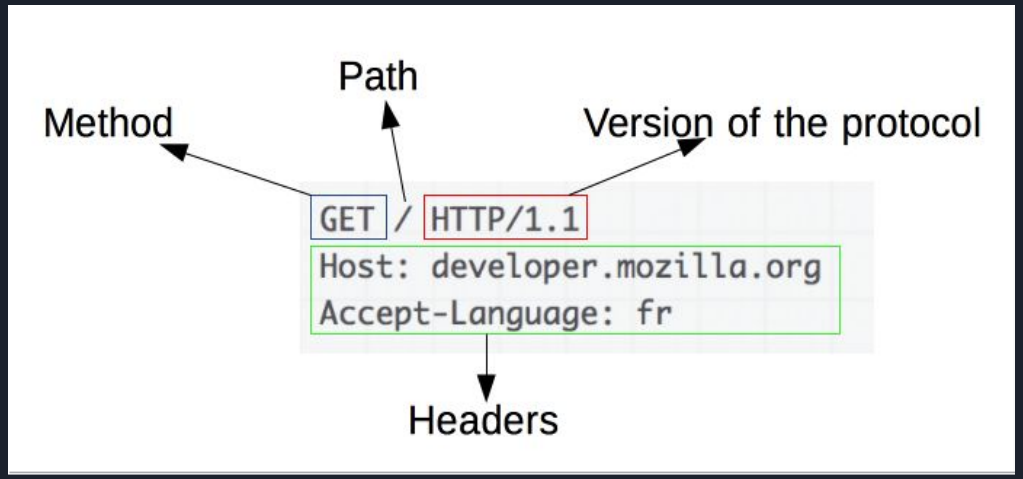
Request é a informação chegando no servidor através do navegador (Input), já o Response é a informação chegando no navegador através do servidor (Output). Com eles é possível ler diversos dados técnicos que podem ser utilizados no desenvolvimento de funcionalidades de aplicações mais complexas, outra utilização bem clássica é analisar se um servidor está respondendo satisfatoriamente as requisições dentro de um período de tempo hábil, por exemplo.

https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Status



Entendo o Request

O protocolo HTTP é baseado em requisições e respostas entre clientes e servidores. O cliente — navegador ou dispositivo que fará a requisição; também é conhecido como user agent — solicita um determinado recurso (resource), enviando um pacote de informações contendo alguns cabeçalhos (headers) a um URI ou, mais especificamente, URL. O servidor recebe estas informações e envia uma resposta, que pode ser um recurso ou um simplesmente um outro cabeçalho.



Métodos de um Request

Quando você vai fazer uma requisição, é preciso que você especifique qual o método será utilizado. Os métodos HTTP, também conhecidos como verbos, identificam qual a ação que deve ser executada em um determinado recurso. Existem 8 métodos HTTP, mas apenas 5 são mais utilizados: GET, POST, DELETE, PUT, HEAD

Entendendo o Response

Nos cabeçalhos de resposta, você pode obter algumas informações muito importantes, dentre elas o código de resposta (Status). Este código identifica se uma requisição foi concluída com sucesso (200) ou se ela não existe (404), por exemplo, mas existem muitos outros.

https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Status

STATUS do Response

- 200 OK - A requisição foi bem sucedida.
- 301 Moved Permanently - O recurso foi movido permanentemente para outra URI.
- 302 Found - O recurso foi movido temporariamente para outra URI.
- 304 Not Modified - O recurso não foi alterado.
- 401 Unauthorized - A URI especificada exige autenticação do cliente. O cliente pode tentar fazer novas requisições.
- 403 Forbidden - O servidor entende a requisição, mas se recusa em atendê-la. O cliente não deve tentar fazer uma nova requisição.
- 404 Not Found - O servidor não encontrou nenhuma URI correspondente.
- 405 Method Not Allowed - O método especificado na requisição não é válido na URI. A resposta deve incluir um cabeçalho Allow com uma lista dos métodos aceitos.
- 410 Gone - O recurso solicitado está indisponível mas seu endereço atual não é conhecido.
- 500 Internal Server Error - O servidor não foi capaz de concluir a requisição devido a um erro inesperado.
- 502 Bad Gateway- O servidor, enquanto agindo como proxy ou gateway, recebeu uma resposta inválida do servidor upstream a que fez uma requisição.
- 503 Service Unavailable- O servidor não é capaz de processar a requisição pois está temporariamente indisponível.

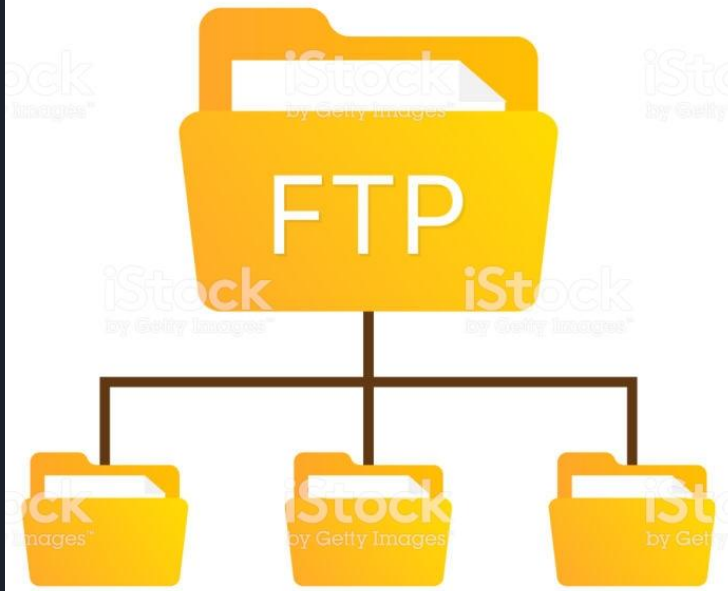
Protocolo FTP

Subsequente / Superior - IFBA

Protocolo FTP

É o protocolo de transferência de arquivos (File Transfer Protocol) realizado entre dois hosts, sendo um cliente e o outro um servidor. Assim como o HTTP, esse protocolo se baseia na conexão IP, usa o TCP e se encontra na camada de aplicação.

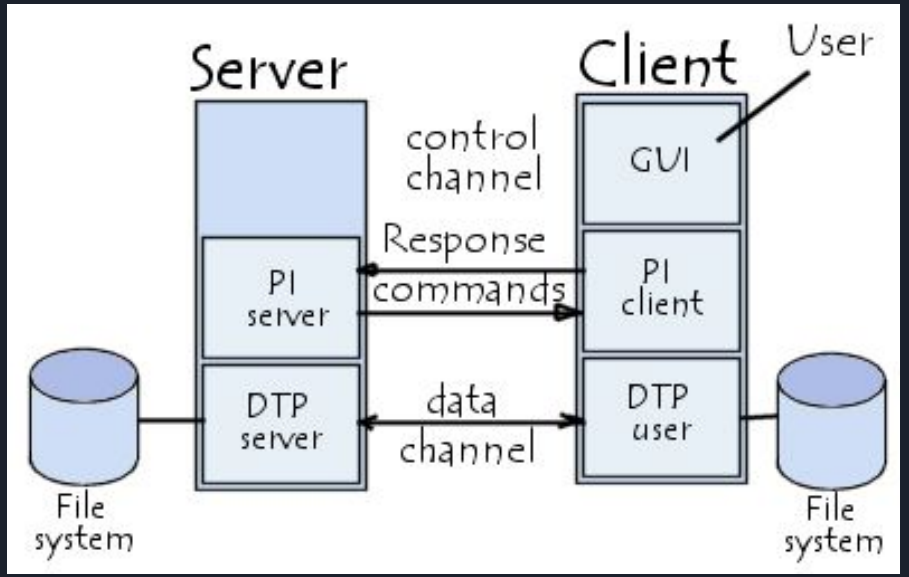
É um protocolo antigo, criado para solucionar o compartilhamento de arquivos em redes TCP/IP ou outros modelos anteriores.



Comunicação FTP

O FTP contém uma característica peculiar de transferência de dados, pois usa duas conexões (uma de controle e outra de dados) separadas em diferentes portas:

- Transferência de dados realizada pela porta 20
- Transferência de informação de controle realizada pela porta 21



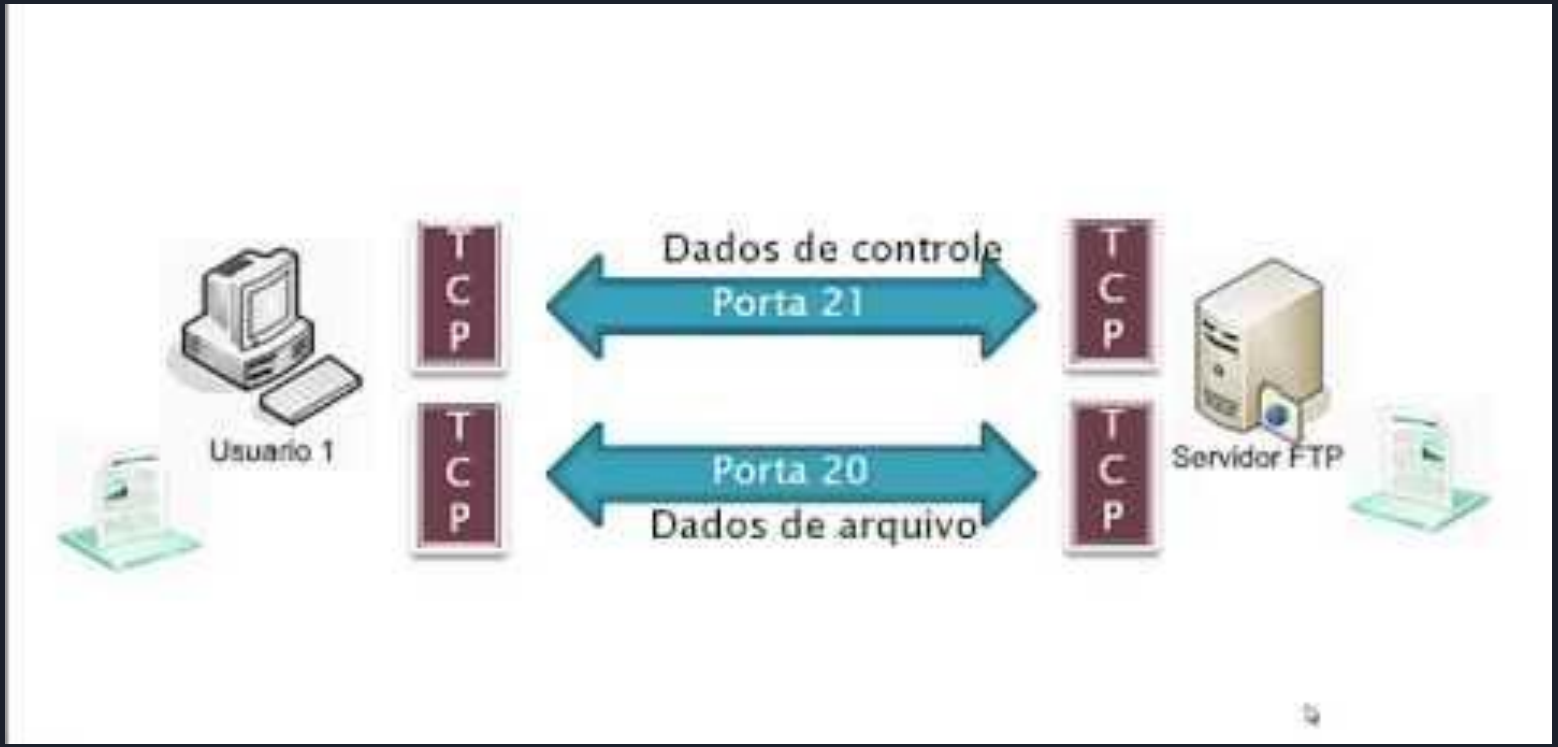
Cliente e Servidor

O cliente é o computador que solicita a conexão para ter acesso aos dados já hospedados na internet. Já o servidor é um outro computador que atua como um ambiente virtual, recebendo a solicitação do cliente para a transferência dos arquivos nele hospedados.

O computador que atua como cliente consegue acesso aos arquivos hospedados na internet através de um programa que se conecta ao computador que atua como servidor. É ele quem também faz a transferência dos arquivos do computador para o servidor.

Já o computador que atua como servidor geralmente possui programas disponíveis para permitir a conexão de computadores externos a ele. Ele simplesmente autoriza a transferência dos arquivos armazenados nele para o cliente que está solicitando o acesso.

Exemplo do FTP



Autenticação de Usuários

- Clientes podem se conectar de forma anônima ou através de usuário e senha. Essas regras dependem da implementação do servidor.
- A conexão e troca de arquivos através do protocolo FTP não está protegida, transferindo arquivos em formato de texto claro, sendo possível a leitura dos pacotes interceptados no tráfego da rede. É possível realizar a proteção de usuários em protocolos que usem SSL/TLS (FTPS) ou SSH (SFTP).

PS.: Falaremos sobre protocolos com camada de segurança, criptografia, chaves de acesso e afins em nossa segunda fase de estudos.

Segurança em FTP

O FTP é um protocolo simples de transferência de arquivos e foi projetado em uma época em que o foco não era a segurança dos dados em si. Isso acaba tornando o protocolo sujeito a ataques de sniffing, spoofing e outros que podem interceptar os pacotes em rede. Dentre as falhas, está o fato que o FTP não criptografa dados transmitidos, inclusive login e senha de usuários.

A partir disso, foi criado uma versão mais segura do protocolo, chamada FTPS. Também temos a forma de transmissão por um túnel seguro (SSH) ou a utilização de VPNs.

Login em servidor FTP

Apesar do uso de diversas aplicações gráficas para gerenciamento de acesso a servidores FTP, o acesso pode ser realizado através de um simples navegador ou explorador de arquivos na maioria dos sistemas operacionais. Basta usar o prefixo no endereço ftp:// no lugar do http:// ou https:// para acessar o servidor FTP

- ftp://endereco.com
- ftp://ip

Ou fazer o login repassando os dados de acesso diretamente pla URL:

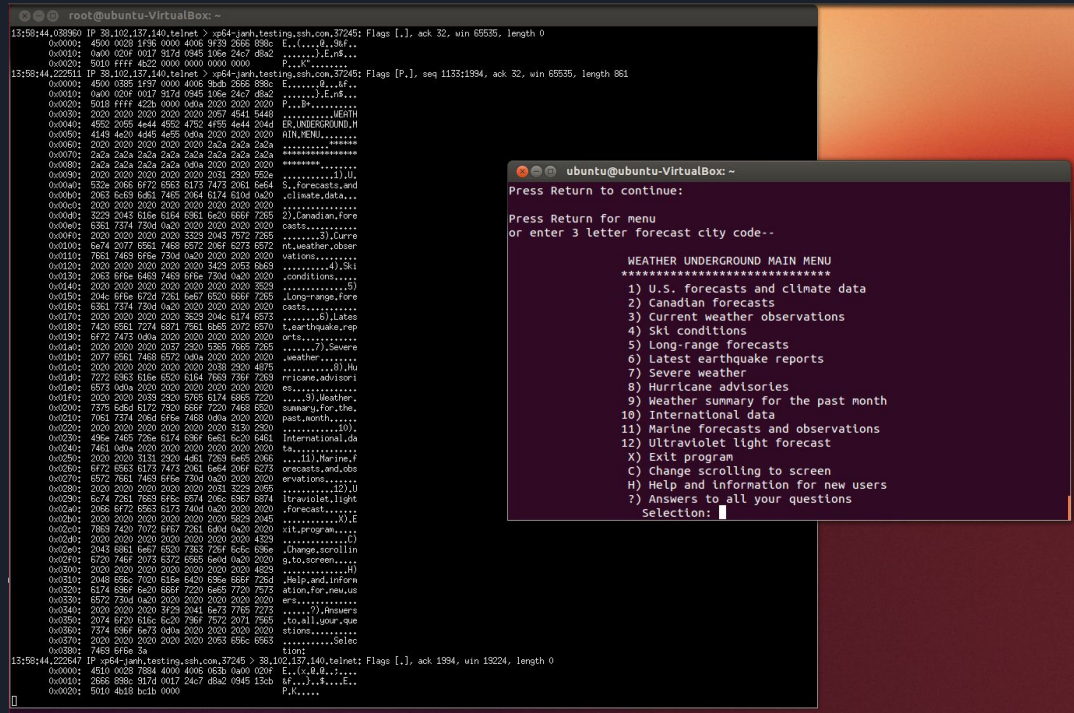
- ftp:// [username] : [password] @ [servidor]
- ftp:// [username] @ [servidor]

Protocolo Telnet e SSH

IFBA - Subsequente e Superior

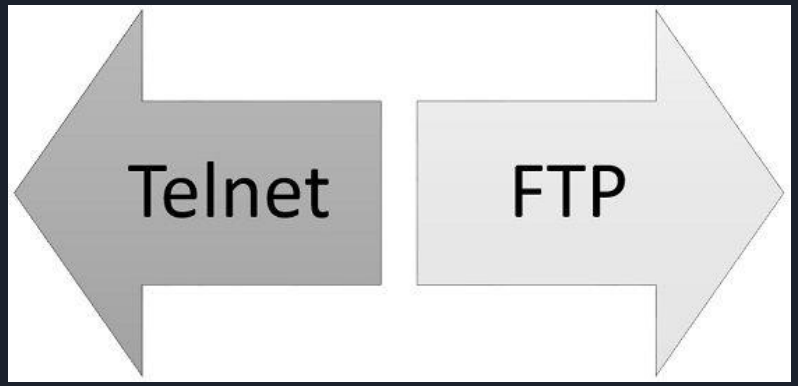
PROTOCOLO TELNET

O protocolo Telnet é um protocolo padrão da Internet que permite obter uma interface de terminais e aplicações pela Internet. Este protocolo fornece as regras básicas para ligar um cliente (sistema composto de uma exibição e um teclado) a um intérprete de comando (servidor).



Telnet vs FTP

Embora a obtenção de um computador remoto por meio de FTP seja comum, o Telnet realmente vai um passo além e permite que você faça logon como um usuário regular do computador, com acesso a todos os dados e programas que possam ser instalados nesse computador. O Telnet normalmente é usado para fins de suporte técnico.



FUNCIONAMENTO PRÁTICO

O Telnet usa um software, instalado em seu computador, para criar uma conexão com o host remoto. O cliente Telnet (software), ao seu comando, enviará uma solicitação para o servidor Telnet (host remoto). O servidor responderá perguntando o nome de usuário e a senha. Se forem aceitos, o cliente Telnet estabelecerá uma conexão com o host, transformando seu computador em um terminal virtual e permitindo que você conclua o acesso ao computador do host. O Telnet exige o uso de um nome de usuário e uma senha, o que significa que você precisa ter configurado uma conta anteriormente no computador remoto. Em alguns casos, contudo, os computadores com Telnet permitirão que convidados façam login com acesso restrito.

SSH vs Telnet

O Telnet não possui nenhuma criptografia. Ele envia as mensagens em texto puro. Dessa forma caso alguém intercepte esses dados conseguirá ver o conteúdo. Mas como um hacker consegue interceptar essas mensagens?

Existem diversas formas de interceptar uma mensagem, ataques como Man in the middle são um exemplo. Outra forma de interceptar essa mensagem é utilizar um farejador (sniffer).

Nos dias de hoje, o SSH é muito mais usado do que o Telnet justamente pelos benefícios da segurança.

Além de ser usado para conectar remotamente, com o SSH nós também conseguimos fazer transferências seguras de arquivos.

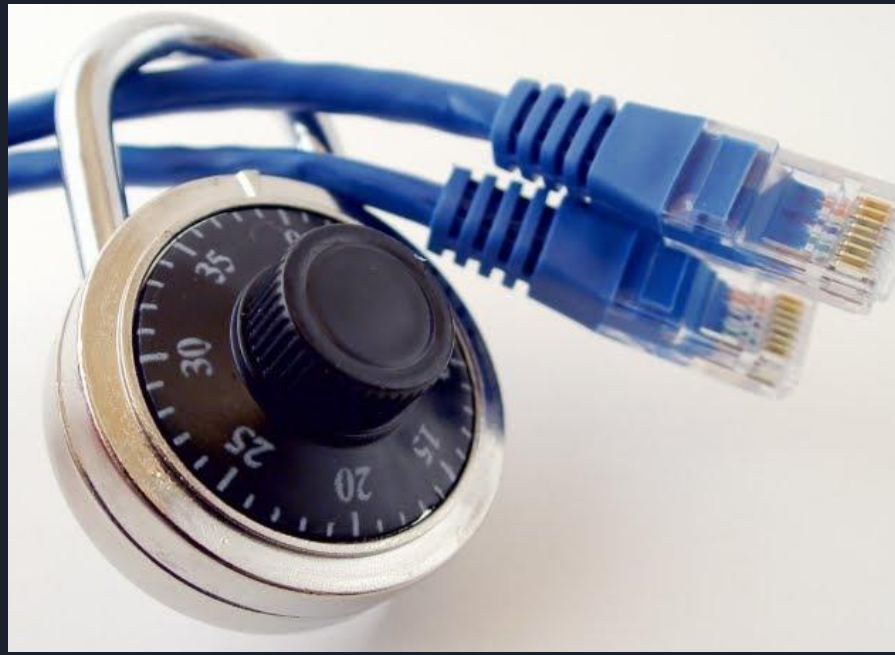
Segurança em Redes

Criptografia e Autenticação

SEGURANÇA EM REDES

Até o momento, estudamos protocolos e serviços que não tem como princípio a segurança de dados. Protocolos como HTML, Telnet e FTP tem como característica a transmissão de texto claro que, uma vez interceptados, são passíveis de análise total de seu conteúdo.

Com a evolução da internet e do poder computacional, surgiu a necessidade de meios de proteção de dados cada vez mais modernos e seguros. Para entender estes mecanismos, precisamos inicialmente compreender os conceitos básicos de criptografia.



CRIPTOGRAFIA

Criptografia é a prática de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de decriptografia específica.

O SURGIMENTO DA CRIPTOGRAFIA

A criptografia nem sempre existiu nos moldes que estudaremos a seguir. Na verdade, ela é quase tão antiga quanto a utilização de idiomas escritos.

Sempre houve a necessidade de criar mecanismos de segurança parque uma informação sigilosa pudesse transitar de forma segura ao seu destinatário. Civilizações antigas contavam com mensageiros ou formas alternativas de envios de mensagens, e necessitavam se assegurar que a informação não pudesse ser compreendida se caísse em mãos erradas. A partir dessa necessidade foram criadas as mais diversas formas de ***criptografia clássica***.

Podemos chamar de criptografia clássica o período que vai desde os povos antigos, passando pela Idade Média e chegando até as máquinas eletro-mecânicas, utilizadas principalmente durante a Segunda Guerra Mundial.

EVOLUÇÃO DA CRIPTOGRAFIA

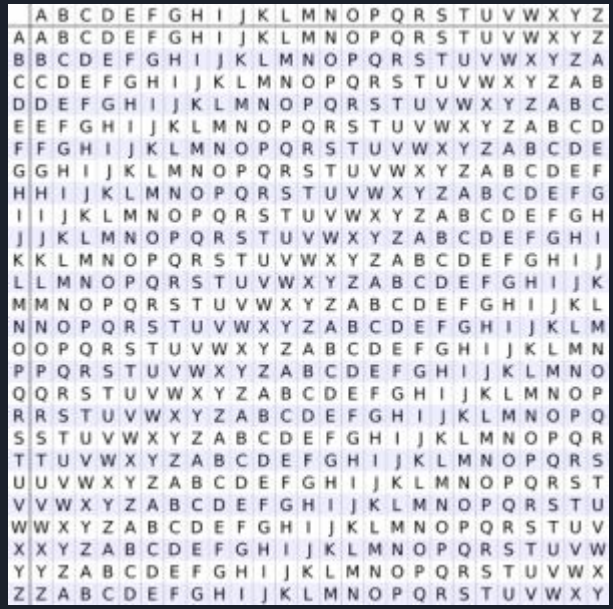
A criptografia vista até o momento era considerada simples e poderia ser facilmente quebrada através de uma análise do texto. Esse modelo é chamado de cifra de substituição, onde cada letra é substituída por uma diferente através de uma chave de codificação.

O problema é que algumas letras se repetem com muita frequência em diversos idiomas, como o “A” e o “O” em nosso idioma. Analisando essa frequência era possível decifrar a mensagem sem ter necessariamente a chave.

Por conta da criação de métodos simples de criptoanálises, cifras de substituição cairam em desuso por alguns séculos.

CIFRA DE VIGENÈRE

A cifra de Vigenère (atribuída equivocadamente a Blaise de Vigenère) foi descrita primeiramente pelo italiano Giovan Battista Bellaso, em 1553, em sua obra La cifra del. Sig. Giovan Batista Bellaso e por muito tempo foi considerada como le chiffre indéchiffrable (a cifra indecifrável) quando, em meados do século XIX, Charles Babbage e Friedrich Kasiki encontraram um método de resolvê-la.



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

CRIPTOGRAFIA MODERNA

A partir do surgimento de computadores modernos, a criptografia evoluiu para o modelo que conhecemos atualmente. Ela herdou muitos dos princípios vistos até agora, como a utilização de chaves criptográficas e técnicas criptoanálises modernas para decifrar códigos.

Para entendimento da criptografia moderna, estudaremos os conceitos de:

- Chave Pública e Chave Privada
- Criptografia Simétrica e Assimétrica.

Criptografia Simétrica

Também chamada de criptografia de chave secreta ou única(ou convencional), utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados. Casos nos quais a informação é codificada e decodificada por uma mesma pessoa não há necessidade de compartilhamento da chave secreta. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave). Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA.

Criptografia Simétrica

- **Me = Fe(M, K)** - Essa é a função genérica para criptografia de simétrica de mensagens. Esse será o funcionamento básico do processo de encriptação, independente do algoritmo utilizado.
- **M = Fd(Me, K)** - Essa é a função genérica para decodificação de mensagem. Esse será o funcionamento básico do processo de decodificação, independente do algoritmo utilizado.

Me = Mensagem Encriptada, M = Mensagem original, K = Chave, Fe = Função de cifragem, Fd = função de decodificação.

Criptografia Assimétrica

Também conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não-repúdio. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um smartcard ou um token. Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ECC e Diffie-Hellman.

Simétrica vs Assimétrica

A criptografia de chave simétrica, quando comparada com a de chaves assimétricas, é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento é mais rápido. Todavia, quando usada para o compartilhamento de informações, se torna complexa e pouco escalável, em virtude da:

- necessidade de um canal de comunicação seguro para promover o compartilhamento da chave secreta entre as partes (o que na Internet pode ser bastante complicado) e;
- dificuldade de gerenciamento de grandes quantidades de chaves (imagine quantas chaves secretas seriam necessárias para você se comunicar com todos os seus amigos).

A criptografia de chaves assimétricas, apesar de possuir um processamento mais lento que a de chave simétrica, resolve estes problemas visto que facilita o gerenciamento (pois não requer que se mantenha uma chave secreta com cada um que desejar se comunicar) e dispensa a necessidade de um canal de comunicação seguro para o compartilhamento de chaves.

Chave Pública e Privada

Na criptografia de chave pública, são geradas uma chave pública e uma chave privada para um aplicativo. Os dados criptografados com a chave pública podem ser decriptografados apenas com a chave privada correspondente. Da mesma forma, os dados criptografados com a chave privada podem ser decriptografados apenas usando a chave pública correspondente. Apenas o proprietário pode acessar a chave privada para decriptografar mensagens que estão criptografadas com a chave pública correspondente.

SUA CHAVE PÚBLICA

Sua chave pública não é como uma chave física, porque ela é compartilhada. Fica em um diretório on-line, onde as pessoas podem procurá-la e baixá-la. As pessoas usam sua chave pública, juntamente com o GnuPG, para criptografar e-mails que enviam para você.

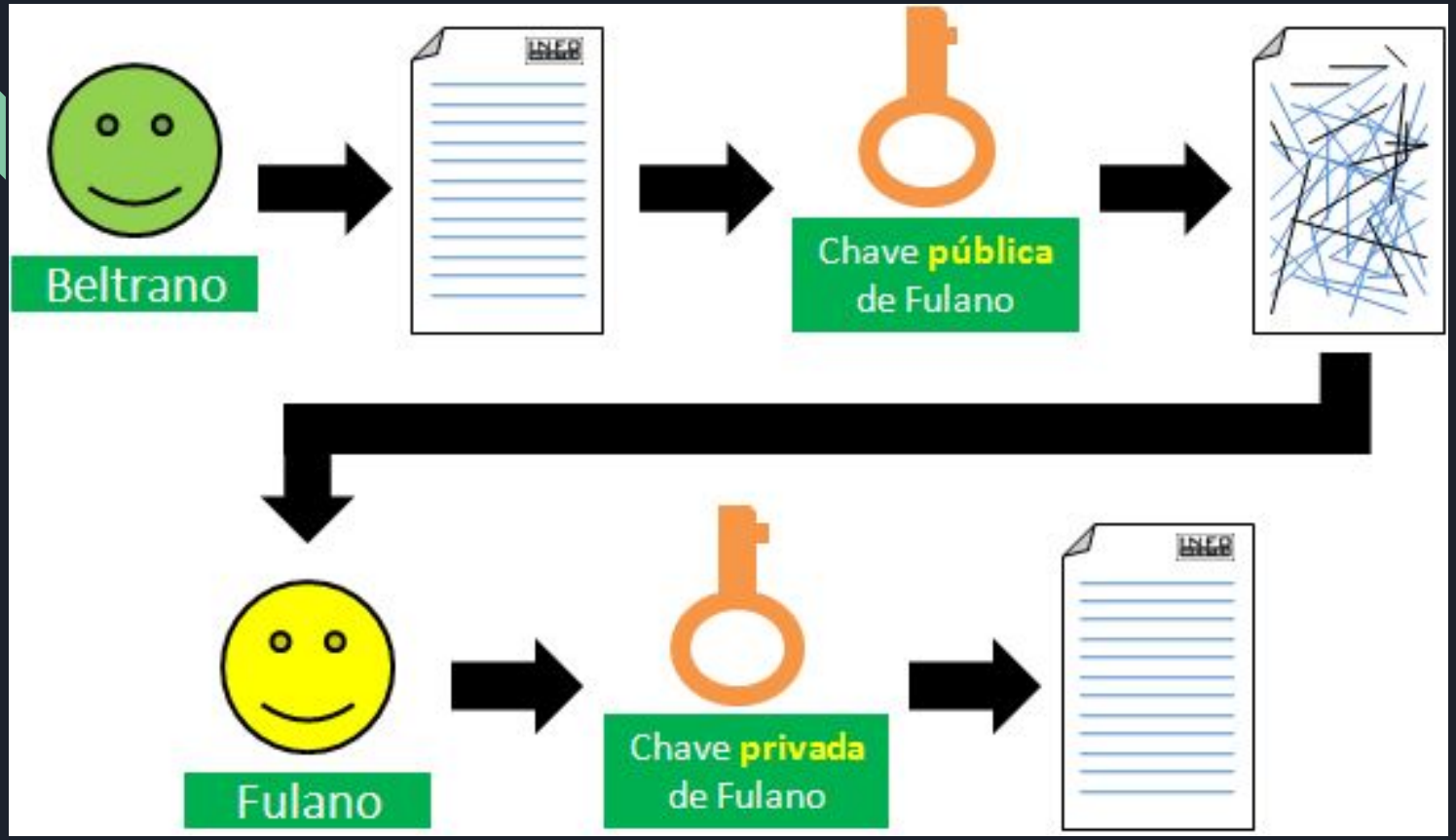
SUA CHAVE PRIVADA

Sua chave privada é mais parecida com uma chave física, porque você a guarda para si (em seu computador). Você usa o GnuPG e sua chave privada para decodificar e-mails criptografados que outras pessoas enviam para você.

Funcionamento Prático

O emissor que deseja enviar uma informação sigilosa deve utilizar a chave pública do destinatário para cifrar a informação. Para isto é importante que o destinatário disponibilize sua chave pública, utilizando, por exemplo, diretórios públicos acessíveis pela Internet.

Por exemplo, para Alice compartilhar uma informação de forma secreta com Beto, ela deve cifrar a informação usando a chave pública de Beto. Somente Beto pode decifrar a informação pois somente Beto possui a chave privada correspondente.


Beltrano
Chave pública de Fulano
Fulano
Chave privada de Fulano