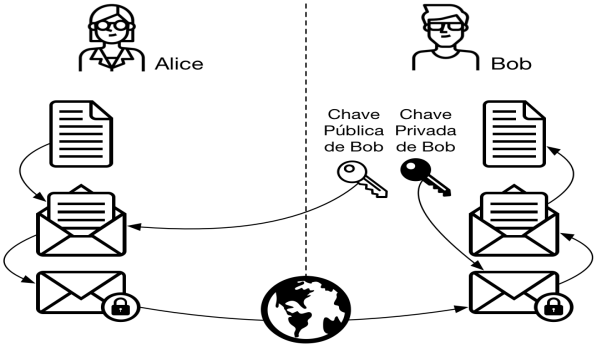


CONCEITOS DE CRIPTOGRAFIA	CONCEITOS DE CRIPTOGRAFIA
O que é Criptografia ?	Criptografia : é uma palavra de origem grega, onde temos a junção de 2 verbos gregos: " Kriptos " (Esconder) e " Grafia " (Escrever), ou seja, a criptografia é o ato de " Escrever Escondido ", ou Cifrar , nos computadores fazemos isso por através de um processo matemático onde trocamos as palavras e letras do idioma comum por caracteres embaralhados que escondem a verdadeira informação e só é possível acessá-la por através de chaves e algoritmos que fazem o processo de Descriptografia ou Decifragem .
O que é Descriptografia ?	Descriptografia : ou Decifragem, é o processo contrário da Criptografia. Enquanto a criptografia embaralha as palavras e números para ficarem ilegíveis, a descriptografia utiliza-se de uma chave (algoritmo que descriptografa a mensagem) transformando os caracteres ilegíveis em palavras e caracteres legíveis para a língua comum .
Ilustre os processos de Criptografia e Descriptografia	
Quais são os tipos de Criptografia existentes?	<p>Temos 2 tipos de Criptografia</p> <ul style="list-style-type: none">- Criptografia de Transposição e de Substituição;- Criptografia Simétrica;- Criptografia Assimétrica;- Criptografia de Curvas Elípticas;
O que seria a Criptografia Simétrica ?	<p>Criptografia Simétrica: Também chamada de "Criptografia de Chave Secreta", é uma criptografia que usa apenas uma chave tanto para cifrar quanto para decifrar mensagens. O usuário responsável por criptografar as mensagens irá usar uma chave criptográfica, que vai embaralhar a mensagem e irá repassar essa mesma chave para que outra pessoa possa decifrar a mensagem usando a mesma chave. A criptografia Simétrica utiliza, em sua maioria a fatoração de números primos para fazer a cifragem dos números, isso graças a aleatoriedade gerada pelo conjunto de números primos.</p> <p>*Números Primos: Um número que só é dividido por 1 e por ele mesmo;</p>
O que seria a Criptografia Assimétrica ?	<p>Criptografia Assimétrica: Também conhecida como "Criptografia de Chave Pública" utiliza 2 chaves, uma delas é só para cifrar uma mensagem e a outra é só para decifrar a mensagem. A chave usada só para cifrar a mensagem é a que chamamos de "Chave Privada", enquanto a chave para decifrar é a que chamamos de "Chave Pública". A criptografia Assimétrica utiliza, em sua maioria a fatoração de números primos para fazer a cifragem dos números, isso graças a aleatoriedade gerada pelo conjunto de números primos.</p> <p>*Números Primos: Um número que só é dividido por 1 e por ele mesmo;</p>
O que seria a Criptografia de Curvas Elípticas ?	<p>Criptografia de Curvas Elípticas: Assim como a criptografia assimétrica, a criptografia de curvas elípticas utiliza 2 chaves, porém, os métodos de criptografia são totalmente diferentes. Enquanto as criptografias Simétrica e Assimétrica utilizam fatoração de números primos, a criptografia de Curvas Elípticas usa álgebra de "Corpos Finitos" ou "Corpos de Galóis", um método de cifragem muito mais elaborado e complexo. Além da elaboração de chaves Públicas bem maiores que as chaves de criptografia simétrica e assimétrica.</p>
O que seria uma "Chave" dentro do contexto de criptografia?	<p>Chave: Uma chave é um número ou combinação de caracteres usados para autorizar a cifragem e decifragem um sistema criptográfico. A chave sempre deve ser secreta, somente os usuários autorizados deverão ter a chave tanto para criptografar quanto para descriptografar uma mensagem, pois se a chave cair em mãos erradas um criminoso poderia se passar pelo legítimo remetente de uma mensagem, ao mesmo passo que ele poderia interceptar uma mensagem original e decifrá-la caso possuía a chave de decifragem do sistema.</p>
Como se dá o uso de Chave na Criptografia Simétrica ? E quais as vantagens e desvantagens do seu uso?	<p>Na criptografia Simétrica o usuário remetente de uma mensagem e o destinatário deverão usar A MESMA CHAVE DE SEGURANÇA para cifrar e decifrar uma mensagem, como podemos observar na imagem abaixo...</p>
- reservada para a questão acima -	<p>Vantagens:</p> <ul style="list-style-type: none">- Pode ser usada em via dupla de comunicação;- É bem mais rápida de ser carregada; <p>Desvantagens:</p> <ul style="list-style-type: none">- Vulnerável à ataques, pois uma única chave é compartilhada entre vários usuários aumentando a chance de roubo da chave;

CONCEITOS DE CRIPTOGRAFIA	CONCEITOS DE CRIPTOGRAFIA
Como se dá o uso de Chave na Criptografia Assimétrica ? E quais as vantagens e desvantagens do seu uso?	<p>Na criptografia Assimétrica tanto remetente quando destinatário devem usar um par de chaves para trocar mensagens entre si, essas chaves são:</p> <ul style="list-style-type: none">- Chave Privada: Uma chave que só o usuário original deverá ter. Essa chave serve para 2 objetivos, 1º para gerar uma Chave Pública, que será compartilhada com outros usuários que desejem cifrar mensagens que serão enviadas para ele. 2º para que o próprio usuário - e somente ele - possa decifrar as mensagens enviadas PARA ELE, mesmo que os demais usuários tenham a Chave Pública daquela pessoa, eles não conseguirão abrir as mensagens enviadas para ele, poderão apenas cifrar mensagens e enviá-las.- Chave Pública: É uma chave que o usuário original distribui para os outros, para que eles possam enviar mensagens cifradas para ele, sem essa chave o envio de mensagens para o usuário original se torna impossível. Essa chave é gerada a partir da Chave Privada do próprio usuário original. <p>Podemos ver um exemplo disso na ilustração abaixo...</p>  <p>Vantagens:</p> <ul style="list-style-type: none">- É super segura, pois a Chave Privada de um usuário nunca sai do computador dele, assim, ninguém pode se passar por ele; <p>Desvantagens:</p> <ul style="list-style-type: none">- Exige maior carregamento, por isso perde em velocidade de troca de mensagens;- Não pode ser usada em via dupla, cada usuário do sistema é obrigado a ter o seu próprio par de chaves, do contrário a comunicação se torna impossível;
- reservada para a questão acima -	
- reservada para a questão acima -	
- reservada para a questão acima -	
O que seriam as Criptografias de Transposição e de Substituição ?	<p>Criptografia de Transposição: reorganiza a ordem dos bits, caracteres ou blocos trocando a ordem dos elementos, por exemplo: AMOR poderia ser transformado em OMRA;</p> <p>Criptografia de Substituição: troca os bits, caracteres ou blocos por outros caracteres aleatórios, onde seria preciso descobrir o algoritmo matemático para identificar que caracteres corresponderiam aos caracteres encriptografados. Por exemplo: cifra de César que troca as letras originais por 3 letras á frente, como: AMOR seria transformado em DPRU;</p>
O que é um Criptossistema ?	<p>Criptossistema: Se refere ao Sistema utilizado para criptografar e descriptografar uma mensagem. Por exemplo: HASH, WEP, WPA, Assinatura Digital e etc.</p>
O que é um Cifra de Bloco ?	<p>Cifra de Bloco: é estilo de cifragem projetada para operar em blocos de dados de tamanho fixo. Por exemplo, o HASH é um código de tamanho fixo, se conseguirmos decifrar esse código, automaticamente conseguimos abrir a mensagem.</p>
O que é um Cifra de Fluxo ?	<p>Cifra de Fluxo: é um estilo de cifragem projetada para operar em fluxo contínuo por toda a mensagem. Um bom exemplo disso são mensagens trocadas por whatsapp, todos os caracteres são embaralhados, e é preciso um descifrador contínuo para desembaralhar toda a mensagem não importa quantos caracteres ela tenha.</p>
O que é a Criptoaanálise ?	<p>Criptoaanálise: é a ciência onde pessoas tentam decifrar um criptossistema que gerou uma mensagem ou uma chave de criptografia, com o objetivo de descobrir vulnerabilidades no sistema para decifrá-lo. Para isso, os profissionais em criptoaanálise, precisam estudar o criptossistema e usar de raciocínio analítico e ferramentas matemáticas para tentar quebrar o código de cifragem da mensagem.</p>