Certified Tech Developer
The Ultimate Degree

Glossário de criptografia

O mundo da criptografia aplicada a sistemas é complexo, você encontrará muitos termos neste documento, alguns já mencionados no material de aula e outros novos. A ideia do glossário a seguir, que contém os termos, siglas, siglas e extensões de arquivo associados ao mundo da criptografia, é que você possa baixá-lo e guardá-lo para referência futura.

Termos e siglas

Termo ou sigla	Significado	Definição
Protocolo		Conjunto de regras orientadas para a implementação de criptografia para proteger um cenário específico (por exemplo, TLS, um protocolo que visa proteger a camada de transporte do modelo OSI). Protocolos diferentes implementam cifras diferentes de acordo com suas necessidades.
Algoritmo		Um conjunto ordenado de etapas que permite solucionar um problema específico. No contexto da criptografia, refere-se a uma mecânica para codificar ou criptografar uma mensagem. Existem muitos algoritmos, que variam em seus níveis de segurança e propósitos. Por exemplo, existem algoritmos criptográficos voltados para a confidencialidade, enquanto há outros voltados para a integridade.
Cipher	algoritmos de criptografia	Conjunto de dois algoritmos usados para codificar e decodificar uma mensagem. Também pode ser usado no lugar da palavra "algoritmo".
Cipher suite		Conjunto de cifras para diferentes finalidades. As cifras são colocadas juntas em um "pacote" que resolve diferentes problemas de segurança, nas três pontas da confidencialidade, integridade e autenticação.

Key	Chave	Chave criptográfica usada para criptografar as mensagens a serem trocadas. No contexto da criptografia simétrica, pode ser conhecido por outros nomes, como: • Chave única • Chave secreta • Chave de sessão • Chave compartilhada
Hash		O resultado do envio de dados a um algoritmo criptográfico para verificar a integridade dos dados.
PKI	Public key infrastructure	A infraestrutura que possibilita a emissão de certificados abrange todos os componentes, desde os CAs até os componentes individuais, como os CRLs e os servidores responsáveis por distribuí-los.
CSR		Documento de texto simples usado para solicitar um certificado de uma CA.
CA	Certificate authority	Servidor responsável pela geração de certificados.
CRL	Certificate revocation list	Lista de certificados emitidos por uma CA que apesar de serem válidos, por algum motivo (a chave privada pode ter sido comprometida), a CA os marcou como não mais válidos. Os navegadores da Internet podem ser configurados para verificar a CRL.
Session key		Chave criptográfica assimétrica que é negociada em tempo real em um fluxo criptográfico assimétrico. A criptografia assimétrica é usada como um canal para negociar a chave de sessão que será usada para criptografar a comunicação real.
x509		Padrão que define a forma e a estrutura dos certificados.
Registration authority		Função dentro da PKI responsável por receber CSRs. Normalmente, a função é desempenhada pelo mesmo servidor que desempenha a função CA, mas eles podem ser separados em computadores diferentes.

Extensões de arquivo

Extensão	Uso
.pem	Arquivos de texto simples com estrutura determinada por uma série de cabeçalhos e rodapés que permitem o armazenamento de certificados e chaves criptográficas para fins de distribuição.
.csr | .req	Arquivos que contêm um documento (em texto simples) com os dados para solicitar um certificado de uma entidade certificadora.
.key	Arquivo no formato PEM que contém apenas uma chave privada.
.crt | .cer	Um certificado emitido por uma CA.
.pfx	Formato que permite que um certificado e uma chave privada sejam agrupados em um único arquivo.
.crl	Arquivo contendo a lista de certificados rejeitados emitidos por uma CA.