TURMA	INTEGRADO/IFRN NOVA CRUZ (INFORMATICA)			**DISCIPLINA**	ARQ. REDES
PERÍODO	2014.1	**ANO**	3°	**PROFESSOR**	HELBER WAGNER
REF	ATIVIDADE-PESQUISA-ARQREDES				

ATIVIDADE DE PESQUISA

SEGURANÇA DE REDES: ALGORITMOS DE CRIPTOGRAFIA

(CHAVE DE RESPOSTA DO PROFESSOR)

Em um ambiente de rede de computadores, um usuário remetente espera que uma mensagem seja transmitida com segurança, e que somente o destinatário legítimo seja capaz de acessá-la. Uma das principais estratégias para a comunicação segura em redes de computadores é a criptografia. Embora os conceitos de criptografia sejam antigos, as técnicas criptográficas permitem que o remetente “disfarce” os dados para tentar impedir que um atacante (usuário não autorizado) acesse a mensagem original, violando a sua confidencialidade.

A mensagem original, criada pelo remetente, é chamada de texto aberto. No remetente, um algoritmo de criptografia recebe, como entrada, o texto aberto, e retorna, como saída, outra mensagem, chamada de texto cifrado. Essa mensagem então é transmitida através da rede, dificultando que um atacante recupere a mensagem original. No destinatário, um algoritmo de decriptação recebe, como entrada, o texto cifrado, e retorna, como saída, o texto aberto, finalizando assim o processo de comunicação segura entre o remetente e o destinatário.

Um elemento fundamental usado para cifrar o texto aberto e decifrar o texto cifrado é a chave. Ela é definida como uma cadeia de caracteres ou números, sendo considerada como parâmetro de entrada pelo algoritmo de criptografia (no remetente) e pelo algoritmo de decriptação (no destinatário). O algoritmo de criptografia usa uma chave e o texto aberto para produzir o texto cifrado. Já o algoritmo de decriptação usa uma chave e o texto cifrado para recuperar o texto aberto.

Existem dois sistemas de criptografia, conhecidos como sistema de chaves simétricas e sistema de chaves públicas. No sistema de chave simétrica, as chaves do remetente e do destinatário são idênticas e secretas. Já no sistema de chaves públicas, são usadas duas chaves: uma pública (conhecida por qualquer usuário) e outra privada, conhecida pelo remetente ou pelo destinatário (mas não por ambos).

Um problema dos sistemas de chave simétrica é que o remetente e o destinatário precisam definir a chave secreta a ser compartilhada entre eles. Contudo, em um ambiente de rede de computadores, essa definição não é trivial, dificultando o funcionamento desse tipo de sistema de criptografia. Essa limitação foi considerada pelos especialistas, que definiram os sistemas de chaves públicas. Nesses sistemas, o destinatário possui duas chaves: uma delas é pública, conhecidas por qualquer usuário, e a outra é privada, conhecida apenas pelo destinatário.

A comunicação usando um sistema de chaves públicas ocorre como se segue. O remetente executa o algoritmo de criptografia, que usa a chave pública do destinatário e o texto aberto para produzir o texto cifrado. Esse texto cifrado então é transmitido através da rede até alcançar o destinatário. Nesse ponto, o destinatário executa o algoritmo de decriptação, que usa a chave privada (do destinatário) e o texto cifrado para produzir o texto aberto, isto é, a mensagem original. Com essa estratégia, o remetente é capaz de enviar uma mensagem segura sem a necessidade da definição prévia de chaves com o destinatário. Embora simples, os sistemas de criptografia de chaves públicas possuem aspectos que devem ser considerados para funcionar adequadamente, incluindo a escolha das chaves e dos algoritmos (de criptografia e decriptação) usados pelo remetente e pelo destinatário.