Segurança da Informação - Prova 2
Prof. Márcio Moretto Ribeiro

Mirela Mei - 11208392

1. **O protocolo MTProto é utilizado no aplicativo Telegram quando as partes optam por se comunicar por meio de um "chat seguro". Dentre as várias opções heterodoxas usadas no protocolo está o uso do modo "encrypt-and-mac" para garantir confidencialidade, autenticidade e integridade. Vimos na aula que o modo "encrypt-then-mac" possui vantagens sobre suas alternativas (em particular sobre o modo usado pelo Telegram). Descreva o modo "encrypt-then-mac" e enuncie as vantagens teóricas que esse modo possui.**

   R: O 'encrypt then mac' utiliza criptografia autenticada, ou seja, é útil para proteger um sistema mesmo que o adversário tenha acesso a um "oráculo" para consultar como determinadas cifras seriam decifradas. Um sistema autenticado de criptografia é a união de um esquema de criptografia com um sistema de autenticação e o encrypt then mac combina esses dois, definindo que devemos primeiro criptografar, e depois gerar o código da cifra.
   Consiste, portanto, em criptografar utilizando um sistema de criptografia $\pi_E = <Gen_E, E, D>$ e em seguida gerar um código de autenticação gerado por um sistema de autenticação $\pi_M = <Gen_M, Mac, Ver>$, gerando o seguinte sistema de criptografia autenticada:

   - $Gen\ (1^n) := k = <k_E, k_M>$ em $Gen_E\ (1^n) := k_E$ e $Gen_M\ (1^n) := k_M$.
   - $E(k, m) := <c, t>$ em que $E(k_E, m) := c$ e $Mac(k_M, c) := t$.
   - $D(k, c) := \{ D\ (k_E, c)$ se $Ver(k_M, c, t)$ ou $\perp$ caso contrário.

   Caso esse sistema seja seguro contra ataques chosen plain-text e o sistema de autenticação seja seguro contra falsificação, o sistema gerado é seguro contra ataques chosen cypher-text (CCA). O modo utilizado pelo Telegram (encrypt-and-mac) não garante segurança contra ataques CCA, portanto essa é a grande vantagem do encrypt then mac.

2. **Prova de trabalho é uma medida para garantir que um determinado usuário tenha que executar uma certa quantidade de processamento**

durante a execução de um protocolo. Essa ideia é usada na mineração de bitcoins e para evitar spams. No segundo caso, brevemente, a ideia é exigir uma quantidade mínima de processamento para um cliente que envie um email. Essa quantidade é desprezível para quem manda algumas dezenas de emails por dia, mas é muito cara para quem deseja mandar milhões de spams. Uma forma de prova de trabalho é entregar para o cliente a saída de um hash e pedir para que ele compute uma entrada que produza aquela saída. Argumente que, se a função de hash escolhida é segura contra colisão, o melhor que o cliente pode fazer é gerar valores aleatórios de entrada até encontrar um cuja a saída coincida com o resultado esperado.

R: A colisão ocorre quando duas entradas diferentes geram o mesmo hash. Assim, se quisermos um sistema que garanta a segurança equivalente a uma função aleatória com chave de 128 bits, precisamos usar uma função de hash muito confiável que produza uma saída com pelo menos 256 bits. A maioria das funções de hash seguem uma construção chamada Merkle-Damgård que assume a existência de uma função de compressão resistente à colisão para mensagens de tamanho fixo e a estende para mensagens de tamanho arbitrário. Construir uma função de hash resistente a colisão para uma mensagem de tamanho arbitrário se resume, portanto, a encontrar uma para mensagem de tamanho fixo que a comprima pela metade.
Partindo desse pressuposto, e visto que a função hash é unidirecional, ou seja, é impossível pegar um valor de hash, aplicar uma função inversa e obter o dado de entrada, não há nada que pode ser feito para tentar quebrar de outras formas. Portanto, a força bruta seria a melhor opção para o cliente, que pode escolher fazer isso por meio do ataque de dicionário ou do rainbow table.

3. **Considere as estruturas ⟨Zn, +⟩ formadas pelo conjunto Zn := {0, . . . , n − 1} e a operação de soma (+) módulo n. Mostre que essa estrutura é um grupo cíclico para qualquer valor de n ≥ 1 e que o número 1 é sempre um gerador nesses grupos. (Dica: Você precisa mostrar que a operação satisfaz fecho, associatividade, possui elemento neutro e inverso. Depois você deve mostrar que o elemento 1 gera todos os elementos do grupo.) Explique porque o grupo ⟨Zn, +⟩ não é um bom candidato para ser usado no protocolo de Diffie-Hellmann.**

R: 1. fecho: para qualquer a, b ∈ Zn tem-se que 0 ≤ a + b (mod n) ≤ n -> a + b (mod n) ∈ Zn
2. associatividade: a soma módulo n satisfaz associatividade, então para todo a, b, c ∈ Zn tem-se que (a + b) + c ≡ a + (b + c) (mod n)
3. elemento neutro: o zero funciona como elemento neutro, pois para qualquer a ∈ Zn tem-se que a + 0 ≡ 0 + a ≡ a (mod n) inverso: para todo a ∈ Zn temos que a + (n − a) ≡ 0 (mod n), como n − a ∈ Zn tem-se que (n − a) é o inverso de a.
4.⟨1⟩ := {0, 1, 1 + 1, 1 + 1 + 1, . . . n − 1} = Zn -> Ao analisar, 1 gera todos elementos do grupo e, por definição, o grupo é cíclico.
Esse grupo não é adequado para ser usado no protocolo de Diffie-Hellman, pois o problema do Logaritmo Discreto é um problema fácil.

4. **O protocolo Pretty Good Privacy (PGP) criado nos anos 90 e usado até hoje utiliza o esquema de certificação baseado em rede de confiança. Explique com suas palavras o que é um certificado digital e como funciona o modelo de rede de confiança.**

R: Uma assinatura digital funciona como um documento que garante identificar o dono de uma chave pública. Consiste em um gerador, que recebe um parâmetro de segurança (sk) e produz um par de chaves (pk), sendo a primeira sigilosa e a segunda pública; um Sign, que recebe a chave secreta sk e uma mensagem m e produz uma assinatura t; Ver, que recebe a chave pública pk, uma mensagem m e uma assinatura t que verifica se essa assinatura é válida para a mensagem e da pessoa que possui a chave secreta. Um certificado digital, portanto, é basicamente um arquivo assinado digitalmente por uma autoridade certificadora associando a identidade do dono com sua chave pública. No modelo rede de confiança, qualquer um pode emitir certificado cabendo aos usuários estabelecer a confiança dessas múltiplas entidades certificadoras, O seu modelo de confiança descentralizado é uma alternativa ao modelo de confiança centralizado de uma infraestrutura de chave pública (PKI), que depende exclusivamente de uma autoridade de certificação (ou uma hierarquia de tais autoridades). Como ocorre com redes de computadores, existem muitas redes de confiança independentes, e qualquer usuário (através do seu certificado de identidade) pode ser uma parte, e uma ligação, entre várias redes.