Sem Consulta

Questão 1)

a) Porque é que no algoritmo 3DES o 2º processamento é uma operação de decifra DES e não de cifra DES ? Justifique adequadamente a sua resposta.

b) No modo ECB usado em criptografia simétrica, se houver um erro na transmissão de um bloco cifrado entre o emissor e o receptor, só o bloco *plaintext* correspondente será afectado. Contudo, no caso de CBC a situação é mais complicada para efeitos de recuperação pelo receptor face à ocorrência deste tipo de erro.

   B1) Que blocos plaintext serão afectados ou corrompidos por esse erro ?
   B2) Supondo que havia também um erro por alteração de um bit nua posição qualquer do bloco Pi no processamento do lado do emissor, antes deste cifrar a informação e enviar, qual o efeito que isso tem no receptor ?
   B3) Do ponto de vista de recuperação dos anteriores erros, qual o modo que apresenta melhor suporte: CFB ou CBC ?

c) Explique em que consiste ou em que se baseia o funcionamento do modo CTR quando usado com métodos criptográficos simétricos. Na sua resposta deve indicar o tipo de processamento subjacente ao modo CTR e que vantagens associa a este modo quando comparado com ECB ou CBC.

d) Diga em que consiste um ataque temporal (*timming attack*) a um algoritmo criptográfico como o RSA e que tipo de atenção deve ser tida em conta na utilização do algoritmo para minimizar esse tipo de ataque.

e) Que vantagens existem em usar a variante OAEP em vez de PKCS#1 quando se utiliza critpografia RSA ? Até que ponto ou em que condições essas vantagens são de facto mais ou menos importantes ?

f) Pretende fazer-se uma implementação de um protocolo do tipo cliente/servidor, protegendo-se a transmissão nesse protocolo com cifra em cadeia bit-a-bit (*Stream-Cypher*). O protocolo tem que ser capaz de cifrar uma fonte de emissão contínua (em tempo real) que existe do lado do servidor, podendo usar-se apenas um método simétrico de blocos como AES em modo ECB usando uma chave de 256 bits. O cliente tem que conseguir receber o fluxo da stream bit-a-bit, também em tempo real.

   Deve indicar como resolveria o problema da cifra e como resolveria o problema da decifra na recepção. Na sua indicação suponha que a geração de bits do lado do servidor pode ser simulada por uma função F(t) simulando a geração de *streaming* indicada, que gera um bit em cada t microsegundos. Note que a sua solução tem que garantir a possibilidade de emitir a stream real-time bit-a-bit cifrada em tempo real, de modo a poder ser recebida pelo cliente num socket também em tempo real.

Consulta

Questão 2)
Considere que alguém tenta usar o algoritmo de cifra com RSA como a seguir se descreve, tendo como objectivo construir um método de síntese segura de uma mensagem M – método a que passaremos a chamar RSAH.

À parte a consideração sobre uma maior lentidão expectável de um tal processo, quando comparado com a adopção de um método usual de síntese, admita que o objectivo é apenas o de conseguir um bom método de síntese do ponto de vista de robustez em relação a propriedades de segurança.

O método RSAH funcionaria então do seguinte modo:

- A mensagem M é inicialmente desdobrada em blocos Bi
- O primeiro Bloco Bi é então cifrado com uma das chaves de um par RSA, (supondo que as chaves já estavam inicialmente geradas).
- O bloco anterior cifrado é então operado com XOR, com o bloco seguinte (com um esquema do tipo CBC como usado com crifras simétricas).
- O resultado anterior é então cifrado de novo.
- Repete-se sucessivamente o mesmo procedimento até ao último bloco.

Mostre que um tal esquema não permite construir de facto um bom método para uma síntese segura de mensagens. Notar que de acordo com o anterior, tem-se, por exemplo, para os dois primeiros blocos, que:

RSAH (B1, B2) = RSA (RSA(B1) xor B2)

Questão 3)

a) Que vantagens ou desvantagens encontra na adopção de um método de distribuição de chaves como o método de Diffie Hellman, o método de Needham-Schroeder com criptografia simétrica e o método de Needham Schroeder com critpografia assimétrica do ponto de vista de garantias de prevenção de segurança futura perfeita ? Justifique adequadamente e de forma bem fundamentada a sua resposta**.**

b) Como sabe, o método de Diffie-Hellman é susceptível de ataques do tipo homem-no-meio, não garantindo, por si só, autenticação entre os dois principais envolvidos numa troca de chaves. Proponha uma solução para prevenir autenticação complementando o protocolo de Diffie-Hellman com um esquema de autenticação e distribuição de chaves segundo o modelo de Needham-Shroeder com criptografia simétrica de modo a evitar aquele ataque. Na sua solução deve apresentar uma representação da especificação do protocolo, com base num diagrama temporal. Nesse diagrama deve apresentar o fluxo de mensagens do protocolo, a representação rigorosa do conteúdo das mensagens utilizando a notação habitual neste tipo de representações e deve complementar a sua descrição indicando o processamento do protocolo ao nível das entidade em causa (PKC, A e B**).** A sua resposta deve seguir em conta rigorosamente os pressupostos dos métodos de Diffie-Hellman bem como do método do método de Needham-Schroeder com cruptografia simétrica.