1-

a) A propriedade perfect forward secrecy não é garantida usando o processo base com RSA para estabelecimento do master\_secret pois…

b) Embora o Record Protocol possa parecer uma simples aplicação de esquemas de cifra e MAC, há alguns detalhes específicos que o tornam imune a certos tipos de ataque:

Ataque de repetição

Um dos possiveis ataques é o ataque de repetição, onde o atacante observa as mensagens trocadas entre as partes legítimas da comunicação e escolhe reenviar uma ou várias num momento oportuno. Apesar das mensagens estarem protegidas por esquemas criptográficos para os quais o atacante não possui as chaves corretas, o reenvio de uma mensagem capturada poderia ser aceite pelas partes legítimas da comunicação, já que o seu conteúdo foi gerado a partir das chaves adequadas, comprometendo assim a integridade dos dados (já que a porções de informações seriam processadas duas vezes pelo recetor). Para se proteger contra este ataque o TLS usa uma tag de autenticação da mensagem que é computada sobre o seu número de sequência original. Assim, caso o atacante capture a mensagem e, logo em seguida, a repita como se fosse uma nova mensagem com número de sequência incrementado. Quando o recetor a receber, ele realiza a verificação da tag, como este número de sequência é diferente daquele utilizado originalmente na geração da marca, a verificação falha, o que demonstra alguma troca de posição da mensagem.

Ataque de reflexão

Outro ataque é o ataque de reflexão. Onde o atacante intercepta uma mensagem transmitida do endpoint A para o endpoint B e transmite-a no sentido oposto. Como esta mensagem foi legitimamente gerada por A, resultante da aplicação de esquemas criptográficos calculados com chaves corretas, então a mensagem deveria passar pelas verificações de integridade e autenticidade. Para solucionar isto o TLS faz uso de material criptográfico diferente para cada sentido da comunicação. Como as chaves e IV utilizados no sentido de A para B são diferentes daqueles usados no sentido oposto, a verificação da marca de autenticação falhará e A facilmente detetará a tentativa de ataque.

2- A técnica CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) é usada para distinguir entre utilizadores humanos e programas automatizados, como bots. Ela geralmente envolve a apresentação de desafios visuais ou problemas que são fáceis para os seres humanos resolverem, mas difíceis para estes bots. **Incompleta.**

3- Para garantir que o cookie que guarda o token do utilizador não é adulterado por nenhuma autoridade diferente no browser podemos proteger o cookie usando um MAC, caso a assinatura não coincidir no momento de rececão do servidor então o conteúdo do cookie foi alterado. Outra grande proteção contra ataques cross-site scripting é usar cookies com a flag httpOnly, de forma a não ser possível aceder ou alterá-lo por código malicioso JavaScript de outros sites. **Interpretaste mal a pergunta.**

4-

5-

6- Configurações para establecer conexão browser-server:

1. Foram nos dados os ficheiros de chaves do servidor secure-server-17.pem e secure-server-key-17.pem
2. Converter CA1-int.cer-> CA1-int.pem openssl x509 -inform der -in CA1-int.cer -out CA1-int.pem
3. Inserir no browser(cliente) o certificado correspondente usado no servidor CA1-int.cer
4. (**Caso o servidor requira autenticação do cliente**) Inserir…
5. Editar o ficheiro hosts (C:\Windows\System32\drivers\etc\hosts) e adicionar a linha “127.0.0.1 www.secure-server.edu”