**Protocolo de Acordo de Chaves de Diffie-Hellman (DH)**

Alice e Bob têm que concordar sobre dois grandes números:   
 **p** (um número primo) e **g** (um número pseudo-aleatório)  
  
Estes números podem ser **públicos**, assim, **qualquer uma** das partes pode escolher **p** e **g** e dizer ao outro abertamente.

Seja Alice gerar, por um PRNG, um número grande (digamos de 512 bits), chamado **x** como **secreto.** Ela guarda um **xA** = x.

Alice temagora **(p, xA)** que define uma **chave privada** em DH.

Alice calcula **gxA mod p** .Alice tem, então, um **expoente privado** **xA**.

Alice inicia o protocolo do acordo de chave enviando a Bob uma mensagem **yA** = **(gxA mod p)** .

**yA** é um valor transmitido, portanto, público.

Bob tem agora um número grande **gxA mod p** (512 bits) definidona tripla **(p, g, gxA mod p),** a qual foi transmitida para Bob, como a **chave pública** DH de Alice.

Bob escolhe um número **y = xB** secreto.

Bob responde enviando a Alice uma mensagem **yB** = **(gXB mod p).**

Alice calcula **(gXB mod p)xA**

Bob calcula **(gxA mod p)XB**

Pela lei da aritmética modular, ambos os cálculos resultam em   
**gxA yB mod p** .

Alice e Bob, agora **compartilham uma chave secreta**: **K = gxA yB mod p .**

Considere agora o ataque “Man-in-the-Middle”. O protocolo de acordo de chave de Diffie-Hellman não é seguro contra um ataque “Man-in-the-Middle”.

Suponha que Alice e Bob queiram se comunicar e para isso devem gerar uma chave k. Seja Eva um adversário. O ataque de repetição acontece da seguinte forma:

1. Eva se prepara para o ataque, gerando duas **chaves privadas** aleatórias XD1 e XD2 e, depois, calcula as **chaves públicas** correspondentes YD1 e YD2.
2. Alice transmite YA  para Bob.
3. Eva intercepta YA e transmite XD1 para Bob.   
   Bob tem uma chave privada, XD1, de Eva.  
   Eva também calcula K2 = (YA)XD2 mod p .
4. Bob recebe XD1 e calcula K1 = (YD1) XB mod p .
5. Bob transmite YB para Alice.
6. Eva intercepta YB  e transmite YD2 para Alice.  
   Alice tem uma chave pública, YD2, de Eva.  
   Eva também calcula K1 = (YB)XD1 mod p .
7. Alice recebe YD2 e calcula K2 = (YD2) XA mod p .

Neste ponto, Bob e Alice acham que compartilham a mesma chave secreta !!!  
  
Mas, Bob e Eva compartilham a chave secreta K1 e Alice e Eva compartilham a chave secreta K2.

Daqui para frente, toda a comunicação futura entre Alice e Bob estará comprometida da seguinte forma:

1. Alice envia uma mensagem M, cifrada por E(K2,M).
2. Eva intercepta a mensagem cifrada e decifra para recuperar M.
3. Eva envia a Bob, a mensagem cifrada E(K1,M) ou E(K1,M’), onde M’ é qualquer mensagem M, modificada.

No primeiro caso, E(K1,M) , Eva simplesmente quer interceptar a comunicação sem alterá-la. No segundo caso, E(K1,M’), Eva modifica a mensagem M, que está sendo enviada para Bob.

Questões:

1. Por que o protocolo de acordo de chaves de Diffie-Hellman é vulnerável a tal ataque com relação aos participantes ?
2. O que se pode fazer para contornar essa vulnerabilidade ?

(C) (Verdade / Falso) Qualquer mensagem pode ser criptografada com   
 algoritmo do acordo de Diffie-Hellman.