UNIVERSIDADE
FEDERAL DO CEARÁ
CAMPUS DE CRATEÚS

Trabalho 02

Criptografia • RSA • 2023.1

Organização das pessoas

- O trabalho será realizado em equipe, as quais devem ser formadas por seis membros (pode ser a mesma equipe do trabalho anterior).
- Cada equipe deve se dividir em duas, em que três pessoas serão responsáveis por cifrar e as outras três serão responsáveis por decifrar.

Realização do trabalho

1. Processo de cifração

- Uma parte da equipe deve implementar o algoritmo RSA com números primos reduzidos, da seguinte forma:
    - A geração das chaves deve utilizar diferentes tamanhos para os números primos $\boldsymbol{p}$ e $\boldsymbol{q}$, de modo que que seja realizado cinco processos de cifração:
        - 1º processo: $\boldsymbol{p}$ e $\boldsymbol{q}$ devem ser primos de 32 bits.
        - 2º processo: $\boldsymbol{p}$ e $\boldsymbol{q}$ devem ser primos de 48 bits.
        - 3º processo: $\boldsymbol{p}$ e $\boldsymbol{q}$ devem ser primos de 64 bits.
        - 4º processo: $\boldsymbol{p}$ e $\boldsymbol{q}$ devem ser primos de 128 bits.
        - 5º processo: $\boldsymbol{p}$ e $\boldsymbol{q}$ devem ser primos de 256 bits.
    - O algoritmo para geração dos números primos $\boldsymbol{p}$ e $\boldsymbol{q}$ deve ser implementado pelo grupo, baseado em algoritmos já conhecidos na literatura.
    - Em todos os processos, o algoritmo deve cifrar uma mensagem de proximamente 100 palavras.
- Os algoritmos para o processo de cifração poderão ser desenvolvidos em qualquer linguagem de programação.
- Deverá ser registrado o tempo necessário para cifrar a mensagem com cada uma das chaves.
- O grupo responsável pela cifração deverá enviar para o grupo responsável por quebrar a cifra do seguinte: (1) o texto cifrado, (2) o módulo $\boldsymbol{n}$ e (3) o expoente de cifração $\boldsymbol{e}$.

2. Processo de quebra

- De posse das informações recebidas do grupo de cifração, o grupo responsável pela quebra da cifra deve tentar descobrir a chave privada para decifrar o texto cifrado. Para isso, o grupo teve descobrir os fatores primos $\boldsymbol{p}$ e $\boldsymbol{q}$ que geraram as chaves pública e privada.
- O grupo deve implementar um algoritmo capaz de fatorar o módulo $\boldsymbol{n}$ e encontra seus fatores primos $\boldsymbol{p}$ e $\boldsymbol{q}$. O algoritmo de fatoração deve ser implementado com base em algoritmos já conhecidos na literatura.
- Como os números primos são reduzidos, há grande probabilidade que o algoritmo encontre $\boldsymbol{p}$ e $\boldsymbol{q}$. Assim, $\boldsymbol{p}$ e $\boldsymbol{q}$ podem ser usados para encontrar a chave privada. Considerando que o algoritmo para gerar as chaves do RSA é conhecido, basta fazer o processo inverso.

3. Dados a serem coletados

- O grupo deve descobrir a chave usada em todos os processos de cifração, ou seja, a chave de 32 bits até a chaves de 256 bits, e de posse das chaves, decifrar o texto.
- Deverá ser registrado o tempo necessário para encontrar cada uma das chaves privadas. O tempo deve ser contado a parti do momento que o algoritmo inicia a fatoração até o momento em que a chave privada é reconstruída.
- O tempo máximo de espera para que o algoritmo encontre $\boldsymbol{p}$ e $\boldsymbol{q}$ deve ser de 24 horas. Caso o grupo não consiga encontrar os fatores primos de $\boldsymbol{n}$ em até 24 horas o processo deverá ser cancelado e esse fato deverá ser registrado.
- Deverá também ser registrado o tempo necessário para decifrar a mensagem com cada uma das chaves.

4. Observações

- A tabela usada para mapear os caracteres do alfabeto em números inteiros deve ser acordada entre todos os membros da equipe.

5. Orientações para a entrega

- A entrega deverá ser feita por meio de um seminário em sala de aula em **21/06/2023**.
- A apresentação consiste em apresentar os dados coletados, como orientado acima, e discorrer sobre o processo de cifração e de quebra da chave.
- Cada equipe terá até 20 minutos para apresentar.