- Prazo de entrega: ver no https://edisciplinas.usp.br/course/view.php?id=117383
- Resolver *individualmente*. Duas soluções **idênticas** receberão **nota zero**
- Utilize **necessariamente** a linguagem Python
- Manuscritos **não** são corrigidos, recebem nota zero.
- Entregue no sistema e-disciplinas um ÚNICO arquivo chamado EP1Python, comprimido (zip, tar, gz), contendo os arquivos seguintes
  - O seu programa em Python, cada uma das saídas, com a sua solução do EP
  - Um arquivo chamado LEIA.ME (em formato TXT) com:
    - seu nome completo, e número USP,
    - os nomes dos arquivos inclusos com uma breve descrição de cada arquivo,
    - qual computador, e qual versão do Python foram usados (modelo, versão, etc..),
- Coloque comentários no seu programa explicando o que cada etapa do programa significa! Isso será levado em conta na sua nota.
- Faça uma saída clara! Isso será levado em conta na sua nota.
- Não deixe para a última hora. Planeje investir 70 porcento do tempo total de dedicação em escrever o seu programa todo ANTES de digitar o programa. Isso economiza muito tempo e energia.
- A nota será diminuída de um ponto a cada dia "corrido" de atraso na entrega.

Este exercício é sobre implementação dos algoritmos de Assinatura e Verificação Schnorr (página 208 do livro-texto)
Notação: || denota concatenação

Escolha dos parâmetros

1. Supor que exista uma autoridade idônea T que escolhe um primo p tal que $p-1$ é *divisível* por um outro primo q ($|p|= 512$ e $q > 2^{80}$) da seguinte forma (neste EP, *você* é esta autoridade):

- Concatena o seu NUSP até formar um número de 80 bits
- Gera um inteiro primo q de $\boxed{80 \text{ bits}}$ baseado no NUSP concatenado, sendo q o primeiro primo $\geq$ NUSP concatenado. Sugestão: calcular primos com o Algoritmo Miller-Rabin (pg. 139)
- Gera um outro primo p de $\boxed{512 \text{ bits}}$, tal que $p = k \times q + 1$ onde k é um inteiro suficientemente grande

2. T escolhe um elemento b tal que $1 \leq b \leq p-1$ e a ordem multiplicativa de b seja q (***e.g.,*** se g é um gerador $\bmod p$, $b = g^{(p-1)/q} \bmod p$). O seu programa deve *calcular* um g e listar o inteiro b

3. Supor que Alice obtém uma cópia autêntica dos parâmetros de T, (p,q,b), e a chave pública de T que permita a verificação da assinatura de T, $A_T(p,q,b)$ sobre (p,q,b). Neste exercício NÃO é necessário implementar e calcular esse A_T

Escolha dos parâmetros para Alice

1. Para que a assinatura seja compacta, recomenda-se usar uma função espalhamento (*hashing*) $h()$ Adotar SHA3 de 256 bits

2. As informações públicas são p, q, b e escolhe uma identificação única I_A e escolhe uma chave secreta s tal que $1 \leq s \leq q-1$ e *calcula* uma chave pública $v = b^{-s} \bmod p$.

3. Alice escolhe uma chave secreta s tal que $1 \leq s \leq q-1$, e *calcula* $v = b^{-s} \bmod p$.

4. Alice se identifica perante T por um meio convencional e transfere v para T com integridade, e obtém de T um certificado

$$cert_A(I_{Aluno}, v, A_T(I_{Aluno}, v))$$

que associa I_{Aluno} com v.

5. A assinatura $A_T(x)$ sobre x é *qualquer* algoritmo de assinatura da autoridade idônea T, verificável publicamente.

Algoritmo Alice para assinar (O texto legível x está no fim deste enunciado e também no e-disciplinas/moodle)

Os passos para Alice assinar um texto legível x usando a sua chave secreta s são os seguintes:

1. Calcula (escolhe) um inteiro aleatório $r : 1 \leq r \leq q-1$.

2. Calcula $u = b^r \bmod p$, $e = h(x||u)$, e $y = (s \times e + r) \bmod q$. O $h()$ deve ser o SHA3 de 256 bits

3. Assinatura da Alice é (y, e).

Algoritmo Beto para verificar uma assinatura

O algoritmo para Beto (i.e., o seu programa) verificar uma assinatura usando apenas informação pública é como segue:

1. Beto obtém as informações públicas p, q, b, v cuja autenticidade é verificada através da assinatura $A_T()$ da autoridade T.

2. Calcula $z = b^y v^e \bmod p$, e $e' = h(x||z)$. O $h()$ deve ser o SHA3-256 de 256 bits

3. A assinatura é válida se e só se $e = e'$.

Executar os itens seguintes e listar os valores calculados:

1. Calcular e listar o inteiro q de ?? bits e o seu comprimento em bits, com uma linha nova contendo:
"O valor de q de ??? bits é ??? ..."

2. Calcular e listar o inteiro p de ??? bits e o seu comprimento em bits, com uma linha nova contendo:.
"O valor de p de ??? bits é ???... ."

3. Calcular e listar o inteiro gerador g e o seu comprimento em bits, com uma linha nova contendo:.
"O valor de g de ??? bits é ???..."

4. Calcular e listar o inteiro $b = g^{(p-1)/q} \bmod p$, $1 \leq b \leq p-1$ e o seu comprimento em bits, com uma linha nova contendo:.
"O valor de b de ??? bits é ???... "

5. Calcular e listar o inteiro s, a chave secreta, tal que $1 \leq s \leq q-1$, e o seu comprimento em bits, com uma linha nova contendo:..
"O valor de s de ??? bits é ???..."

6. Calcular e listar o inteiro $v = b^{-s} \bmod p$, a chave pública, e o seu comprimento em bits, com uma linha nova contendo:..
"O valor de v de ??? bits é ???...".

7. Calcular e listar o inteiro $r : 1 \leq r \leq q-1$ e o seu comprimento em bits, com uma linha nova contendo:..
"O valor de r de ??? bits é ???..."

8. Calcular e listar o inteiro $u = b^r \bmod p$ e o seu comprimento em bits, com uma linha nova contendo:..
"O valor de u de ??? bits é ???..."..

9. Calcular e listar em ***hexadecimal*** e =SHA3-256$(x||u)$ e o seu comprimento em bits, com uma linha nova contendo:..
"O valor de e de ??? bits em hexadecimal é ???..."..

10. Calcular e listar o inteiro $y = (s \times e + r) \bmod q$ e o seu comprimento em bits, com uma linha nova contendo:..
"O valor de y de ??? bits é ???..."..

11. Calcular e listar o inteiro $z = b^y v^e \bmod p$ e o seu comprimento em bits, com uma linha nova contendo:..
"O valor de z de ??? bits é ???..."..

12. Calcular e listar em ***hexadecimal*** $e' = h(x||z).$ e o seu comprimento em bits, com uma linha nova contendo:..
"O valor de v de ??? bits em hexadecimal é ???..."..

13. Verificar se $e = e'$ e listar uma mensagem consistente.

Texto de entrada:

A presença de estudantes de todas as faixas etárias e classes sociais nos museus da USP possibilita um canal efetivo de diálogo entre a Universidade e a sociedade. Também torna possível um diálogo democrático sobre o nosso passado e sobre a produção de novos saberes, memórias e acervos.” É assim que Aline Antunes Zanatta, educadora do Museu Republicano Convenção de Itu, em São Paulo, destaca a importância do serviço educativo nos museus e centros de cultura e ciência da USP. Ela explica que é esse serviço, que estabelece uma relação com os visitantes a partir de programas educativos, que aproxima o público do universo museal.

Outro espaço de ações educativas, a Matemateca do Instituto de Matemática e Estatística (IME) da USP pretende fazer parte do mapa de visitas culturais da cidade de São Paulo. “Cada vez mais os estudantes da escola básica precisam de estímulos para estudar matemática. Essa é uma necessidade que já existia, mas se intensificou durante a pandemia. A Matemateca, por ser uma iniciativa de divulgação lúdica da matemática, tem um papel fundamental na reversão desse quadro”, explica Eduardo Colli, diretor do acervo de objetos interativos que ajudam a divulgar a matemática.

Além destes, outros museus da USP possuem ações educativas que auxiliam escolas e grupos na tarefa de ampliar o diálogo e produzir novos saberes. Além de visitas mediadas, as instituições oferecem materiais de apoio, como kits, livros e vídeos, inclusive para empréstimos, que podem ser utilizados em sala de aula e para planejamento de visitas presenciais aos acervos. Há também parques, como o Cientec, na Água Funda, em São Paulo, que oferecem passeios e atividades lúdicas para o ensino de ciências, e as Ruínas São Jorge dos Erasmos, em Santos, que propõe visitas a um importante sítio arqueológico da história do Brasil.

Confira abaixo algumas ações educativas de museus da USP e programe a visita de sua escola ou grupo.

Desde sua abertura ao público, ainda no século 19, o Museu do Ipiranga estabeleceu uma relação muito próxima com a educação formal. Muitos visitantes, ao se lembrarem do Museu, o associam justamente a uma visita realizada com a escola, seja na infância ou na adolescência.

Este programa busca estruturar propostas educativas pensadas especialmente para este público: professores e alunos de diversas faixas etárias e etapas de escolarização (Ed. Infantil, Ensino Fundamental, Ensino Médio, Educação de Jovens e Adultos e Ensino Superior).

Para a formação de professores, são oferecidos cursos de formação regulares relacionados às temáticas das exposições do Museu, assim como materiais de apoio às ações educativas desenvolvidas em sala de aula. O objetivo é ampliar canais de diálogo entre o Museu e profissionais de educação de escolas públicas ou privadas, contribuindo para o desenvolvimento de diferentes propostas pedagógicas e fomentando a apropriação das discussões propostas pela instituição a partir de obras de seu acervo. Além disso, busca aproximar e sensibilizar profissionais da educação formal sobre os potenciais educativos do trabalho junto a museus. Os materiais educativos desenvolvidos podem ser acessados abaixo, na área Downloads, e também são distribuídos durante os encontros de formação presenciais.

Para as atividades com estudantes, são oferecidas ações educativas que exploram os espaços expositivos do Museu por meio de recortes temáticos considerando como referência a Base Nacional Curricular Comum. Durante as visitas educativas, educadores do Museu buscam estabelecer diálogos com os grupos trabalhando com propostas que articulam diferentes exposições. Para cada faixa etária há uma proposta educativa distinta e durante a visitação são construídos caminhos de leitura das obras do acervo, em diálogo com os olhares trazidos pelos visitantes.

Para mais informações, entre em contato com a equipe de educação no e-mail serveduc@usp.br.

——————————— FIM ———————————