**Atividade**

Bob quer enviar uma mensagem criptografada para Alice. Ele queria usar criptografia assimétrica, mas estudou que ela é computacionalmente pesada. Então ele teve uma ideia. Gerou uma chave secreta/simétrica e a criptografou com criptografia assimétrica RSA 2048 bits. Com a chave simétrica gerada, ele cifrou a mensagem para Alice, usando o algoritmo simétrico AES CBC 192 bits. Daí, ele formatou a mensagem para Alice. Ele escreveu para Alice que ela poderia recuperar a chave simétrica da mensagem assimetricamente cifrada (em base64):

K6znC0dtNhxE0/cGEi29HzWXpeYnbzp82Lcl3dizFY/EPy+/FI8zLoSZLE5fkPV+htb8678YBlnp3jLiua31BWXCTXVaY7bmgC0HVz3s2Abgnq1tRoj3KymWmqH77pAlOs+358+uagGU5TuzXsrMhGLkV+Q+P3bP8m/bXWGXIH6appSY5sBM0jBsAmPLePKiUj+ggAi5vdCIj9NcDUpBRkPToJ0WfrIiv68DGTTBAAMkbwolGPQeUPl3GC8aGXfwnuHx3MdLkO+XkAf0eW059+b4COLduMAQ0tMpZXF8xEvrBf4tK9pWNNciDkU7DhuXcNX5+nhVq7HrTrG7I8Yn0Q==

Com a chave simétrica, Alice poderia recuperar a mensagem em base64, usando o AES-192 (CBC) e o texto cifrado abaixo (em Hexa):

0E6BC8AD7CB3DC17BD8DD2F4393E0F1C3ACA0A389D03AD435079E51619DA43793282A5ED3F7DFC714D313D8306727A77921C4FDC0E65CF1AB9C033F22B80542231938EE7D03DCC6CA3DCB4426BFD61E6FAD086AEEAC0CCB7629003C3191310AA94A39AF7CAFCE3EB8C79675E45209205CD1C707F83C9EFE7EABED0EC5E9FA678

Alice tem o seguinte par de chaves RSA 2048 bits:

Chave Pública

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlI25dkGP671wKKgnqrdk+uVq0GoYHjQNzLm5gsi1T43RzX9ff0yxJQlB0XiSdhrTj44Hg12zX+qQJL28lYZjwR39OlhSMwa4NmMTMkgpmLHkK6L22F3Xb37k08nfAf+Oh2gTeQgXb+/VpvYnmzRhLXcqbcXuivEgK3y/PUVB3CIZIB8Wf/LTVKmKVj0NUoX0YUXuQp5j7nZ/NadUOJTjMYLLRosDM74U/8Yk6ebluHapJYsFbUbkrXxS9EewuYK/Uvsjjj7hIv8Oj3WnmT2v8gKrEfe+yP7kRInkAuQM+L6r0t3N8cvn+tn/olgtMZo28/c4Jqrtva3RAcyS2uysiwIDAQAB

Chave Privada



O que deveria ter feito Bob para assinar a mensagem?

Para resolver esta questão, use as ferramentas online:

Criptografia Assimétrica com RSA 2048 bits:

https://www.devglan.com/online-tools/rsa-encryption-decryption

Criptografia Simétrica com AES CBC 192 bits:

https://www.devglan.com/online-tools/aes-encryption-decryption

Para recuperar a mensagem em ASCII do texto em Base64: https://www.devglan.com/online-tools/base64-encode-decode