Supplemental Problem for Problem Set #6

Due Friday, October 28, 2016

You and Bob need to exchange messages, and both of you have established your RSA credentials:

Bob's public key is $(720017, 11)$

Your RSA values are $p = 1163$, $q = 1093$, and $e = 17$

However, you are concerned that Bob's keys will become compromised at some point. You request that he send you a new set of credentials (n_1, e_1) for your communications, and he agrees to do so.

S-1. Bob uses your public RSA key to encrypt n_1 and uses his old RSA credentials to sign the encrypted n_1:

$$(x = 271816,\ \text{sig}(x) = 587658)$$

Verify Bob's signature. What is the value of n_1?

S-2. Bob follows the same process to send you e_1:

$$(x = 652572,\ \text{sig}(x) = 97001)$$

Verify Bob's signature. What is the value of e_1?

S-3. Now that you have Bob's new credentials, you are comfortable that your communications will be secure. You need to send him your birth year and month as a six digit number. For example, if you were born in April of 1991, you want to send Bob 199104.

Use Bob's RSA credentials that you determined above to encrypt your message and sign your message using your RSA credentials. What do you send to Bob?