Quiz #4

MATH 481/581 — Cryptography
Monday, Mar 27

Please print your name:

Problem 1. Bob's public RSA key is $N=55$, $e=3$.

(a) Encrypt the message $m=8$ to send it to Bob.

(b) Determine Bob's secret private key d.

Solution.

(a) The ciphertext is $c=m^e \pmod N$. Here, $c\equiv 8^3=8^2\cdot 8\equiv 9\cdot 8\equiv 17 \pmod{55}$. Hence, $c=17$.

(b) $N=5\cdot 11$, so that $\phi(N)=4\cdot 10=40$.

To find d, we compute $e^{-1} \pmod{40}$ using the extended Euclidean algorithm:

$$\begin{aligned} \gcd(3,40) \qquad \boxed{40} &= 13\cdot\boxed{3}+1 \\ = \ 1 & \end{aligned}$$

Hence, $3^{-1}\equiv -13\equiv 27 \pmod{40}$ and, so, $d=27$. □

Problem 2. Bob's public RSA key is $N=33$, $e=17$, and his secret key is $d=13$.

Decrypt the ciphertext $c=6$.

Solution. We need to compute $m=c^d \pmod N$, that is, $m=6^{13} \pmod{33}$.

$6^2\equiv 3$, $6^4\equiv 9$, $6^8\equiv 15 \pmod{33}$. Hence, $6^{13}=6^8\cdot 2^4\cdot 6\equiv 15\cdot 9\cdot 6\equiv 18 \pmod{33}$, so that $m=18$. □

Armin Straub
straub@southalabama.edu