

MATH 445, HOMEWORK 7

1. Your RSA public key (n, e) is $(18923, 1261)$. Factor n and compute your private key. You have been sent the message 12423; decrypt it.

2. Let $p = 31847$, $g = 5$, and $a = 7899$. Compute $b = g^a \pmod{p}$. Consider the ElGamal cryptosystem with (p, g, b) as your public key and a as your private key. You have received the message

$$(3781, 14409).$$

Decrypt it.

3. Using the ElGamal key from the previous problem, sign the message $m = 3920$ using the random number $k = 133$ with the ElGamal signature scheme. Then, verify the signature.

4. Download and install an implementation of SHA-1 (or find an online applet that will compute SHA-1 hashes, or implement SHA-1 yourself) and compute the SHA-1 hash of this PDF.

5. In class, we proved that if q numbers are chosen randomly and independently from the interval $[1, \dots, N]$, then the probability of a collision is at least $1 - e^{-q(q-1)/2N}$. Use this to prove that if

$$q \geq 1 + \sqrt{2N \log \left(\frac{1}{1 - \epsilon} \right)}$$

then the probability of a collision is at least ϵ . Conclude that if $q \approx 1.177\sqrt{N}$ then the probability of a collision is approximately at least $1/2$. What does this estimate give for $N = 365$?