Cryptography

Peter Kelly

September 27, 2023

1. The shared key agreed upon by Alice and Bob is 22. To find this, I examined x when $1 \leq x \leq 50$ for $7^x \text{mod}(61)$. Then when $7^x \text{mod}(61) = 30$ or $7^x \text{mod}(61) = 17$ I knew I had found either Alice's or Bob's private key respectively. Using Alice's and Bob's secret keys, I could then calculate the shared secret key. If A and B were larger, it would be much harder to brute force this since the range of x's you would need to check would be immensely larger.

2. Alice sent Bob the message ăKă8tĝt ĤYiAx ĝSĝSĚRQĝ!ĤğEĚ9ĕ5-ċ(bxOĆĬ¿ĀaĪĝvUĝčXĕ-vWĤWy!ĚğVčbùĶ čZ4Ĭ4ă8yĥčOĕ1Wč'UĝĆ1ù(tù.Uù.ăĪăıKĤcĩ)ğVĝĬ3ĩ))ĩaĈOĥt'ăċi ti ĤĤUi. To encode the message, Alice takes her plaintext bytes, M, and finds $M^e \text{mod}(n)$. To decode her message, I factor n to find p and q then can calculate d since I know e, p, q. Then I can decode the message by finding $M^d \text{mod}(n)$. If the numbers had been larger, it would have been impossible to find p, q from n since prime factorization is only possible for small numbers. Since Alice encoded each message block separately, this encryption would have been insecure as patterns could have continued through the encryption.