

HW 30

1. Define key, secret key, public key.
2. Decipher the following, which uses a Caesar shift cipher.
znkxk oy tu xuegr xugj zk mkuskzxe--kairoj
3. What is a book cipher?
4. Please comment. (G.H. Hardy, *A Mathematician's Apology*, 1940, taken from *A Course in Number Theory and Cryptography*, 2nd ed. by Neal Koblitz)
"...both Gauss and lesser mathematicians may be justified in rejoicing that there is one science [number theory] at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean."
5. What do inverse functions have to do with cryptography?
6. Read the following sites.
<http://www.rsasecurity.com/rsalabs/node.asp?id=2094>
<http://www.rsasecurity.com/rsalabs/node.asp?id=2093>
7. What do you think is the purpose of the RSA Challenge?
8. Please comment. (*The Code Book*, Singh)
"It has been said that the First World War was the chemists' war, because mustard gas and chlorine were employed for the first time, and that the Second World War was the physicists' war, because the atom bomb was detonated. Similarly, it has been argued that the Third World War would be the mathematicians' war, because mathematicians will have control over the next great weapon of war—information."
9. What would you reply to someone who asks, "Hasn't all the math been discovered already?"
10. What are some of today's math areas that the ancient mathematicians did not and could not have?
11. What would you say to someone with the idea that mathematicians sit around and make theorems?

Resource:

<http://www.garykessler.net/library/crypto.html>