CS/ECE/MATH 435: HOMEWORK 10, DUE DEC 7.

1. Which of the following is not traditionally an information source for authenticating someone's identity? Explain.
(a) Something you know.
(b) Something you have.
(c) Something you like.
(d) Something you are.

2. You are given a piece of data. Storage is limited so you also need to compress the data (losslessly, so you can reverse the compression). You are given RSA for encryption and signing and given a good compression algorithm (e.g. LZW).
(a) Should you encrypt first or compress? Or does the order not matter? Why?
(b) Should you sign first or compress? Or does the order not matter? Why?

3. Zero-knowledge proofs are where you convince someone you can do something without actually giving away the proof. For example, suppose Alice wants to convince Bob that she knows a number x without Bob figuring out x (this has applications e.g. in banking).

Here's how she can do it. She picks two large distinct primes p, q and sets $N = pq$. She possesses a number x between 1 and N. She tells Bob N and $x^2 \pmod{N}$ (over a public channel). If Bob could factor N, then he could compute x and it is believed that there is no easier way to find x.

Alice now picks a random integer r and sends Bob $x^2r^2 \pmod{N}$. Bob randomly sends one of two questions - "Send me $r \pmod{N}$" or "Send me $xr \pmod{N}$".
(a) Show that Alice can satisfy both these requests.
(b) Show that Bob can check her answer in either case.
(c) Suppose Oscar tries to fool Bob that he knows Alice's secret x, by making up a random number s and sending s^2 to Bob. Show that if Bob asks for $xr \pmod{N}$, Oscar is OK according to Bob's check in (b), but that if Bob asks for $r \pmod{N}$, then Oscar is caught. Can Oscar answer Bob if Bob asks for $r \pmod{N}$? Why does this mean that by playing this game several times with different r, Alice gives a zero-knowledge proof with high probability.

[Think of Ali Baba's cave.]

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX