Illustrate with numerical examples, with your own choice of parameters

1. El Gamal Signature Scheme
2. Schnorr Signature Algorithm
3. DSA
4. Chaum-van Antwerpen Signature Scheme

To be able to do this we need a hash algorithm too (for Schnorr and DSA). So we will create our own little hash algorithm.

Our hash algorithm goes like this. The input is one or more numbers in \( \mathbb{Z}_q \). The output is one number in \( \mathbb{Z}_q \).

If the input is \( x \in \mathbb{Z}_q \), we calculate the hash as

\[
h(x) = x^l \mod q.
\] (1)

To calculate the hash of more than 1 number, say \( t \) numbers \( x_1 \cdots x_t \in \mathbb{Z}_q \) we define the hash function as

\[
h([x_1 \cdots x_t]) \equiv \prod_{i=0}^t h(x_i) \equiv x_1^l \times \cdots \times x_t^l \mod q \] (2)

(each one of you will hopefully choose a different \( l \) to implement the hash function).

I haven’t covered the last one, Chaum-van Antwerpen, in class yet. I will cover it on Tuesday. The writeup is already there in the latest version of the lecture notes.

**Do not choose parameters identical to the ones in the text!**

On an unrelated issue, the hash algorithm I have chosen has an extremely undesirable property. Can you identify?