1. Has the security of AES itself been proven (in the mathematical sense) ?

2. If we have a truly secure block cipher, can modes of operation be proved to be secure ?

3. Consider the CTR mode with (say) AES: there is a running counter $i$, which is increased for each block. This is used to generate a keystream, which in turn is xored with the plaintext to produce the ciphertext (and vice versa); $C_i = E_k(i) \oplus P_i$. Can you describe the exact security of this mode against a distinguishing attack ? How would such a distinguisher work ?

Note 15.04.04: Sorry, this wasn’t a very well defined question, and when understood in the strictest sense, also very difficult. Partial answers are accepted as long as the basic trick is understood. - mjos