Abstract:
ALGORITHMS are instructions for single agents. PROTOCOLS are instructions for multiple agents. Agents may be specified to be humans or computers.

Our GOAL is to know which cryptographic problems can be solved by protocols that specify certain agents to be human. We are especially interested in the case in which each human does all computations entirely in his/her head (in all dealings with the other agents).

QUESTION: Can a human compute something/anything PRIVATELY -- entirely in his head -- that NO ADVERSARY -- BE IT HUMAN, COMPUTER, OR COMBINATION OF THE TWO -- can reasonably get hold of? In particular, can a human compute a private hash function \( h(x_1), h(x_2), \ldots \)

• with just a few (3?) hours of preprocessing to learn \( h \), and just 1 minute of processing per input \( x_i \) to compute \( h(x_i) \), so that

• a human/computer combo that observes a small number of pairs \( (x_1, h(x_1)), (x_2, h(x_2)), \ldots \) but does not otherwise know \( h \) (because it is private and hard to infer) cannot compute \( h(x) \) on a new \( x \).

EXAMPLE: PASSWORDS.
Definition: A PASSWORD SCHEME is an algorithm for producing passwords in response to given challenges (typically domain names).

THEOREM: there exists a PASSWORD SCHEME that is
1. WELL DEFINED (a mathematical concept),
2. HUMANLY USABLE by a normal dedicated human being, namely me (an experimentally demonstrable concept),
3. MACHINE UNCRACKABLE to a small well-defined extent (as determined by the password game).

Bio:
Manuel Blum, the Bruce Nelson University Professor of Computer Science at Carnegie Mellon University, is a pioneer in the field of theoretical computer science and the winner of the 1995 Turing Award in recognition of his contributions to the foundations of computational complexity theory and its applications to cryptography and program checking, a mathematical approach to writing programs that check their work. A member of the National Academy of Sciences and the National Academy of Engineering, he is a fellow of the American Academy of Arts and Sciences, the American Association for the Advancement of Science, and the Institute of Electrical and Electronics Engineers. Dr. Blum has held a Sloan Foundation Fellowship and received a University of California at Berkeley Distinguished Teaching Award, their Faculty Research Award, the Sigma Xi's Monie A. Feist Award, the Carnegie Mellon Herbert A. Simons Teaching Award, among other honors. He is the author of more than 50 papers published in leading scientific journals and has supervised the theses of 35 doctoral students who now pepper almost every major computer science department in the country. The many ground-breaking areas of theoretical computer science chartered by his academic descendants are legend.