Encryption Experts Call For Much Longer Key Lengths

December 31, 1969

Supporting Documents

Seven leading experts on cryptography have released a joint report arguing that dramatically stronger encryption is needed to provide adequate privacy and security for computer users. The study calls for the deployment of 75- to 90-bit key length encryption systems, in contrast to the 40-bit systems currently exportable under Administration policies. The report, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security" was written by cryptography and computer security experts Matt Blaze, Whitfield Diffie, Ronald Rivest, Bruce Schneier, Tsutomo Shimomura, Eric Thompson, and Michael Weiner. The study joins the mounting body of evidence showing that products exportable under the Clinton Administration's encryption policies do not provide adequate privacy and security. The report argues that computer products with 40-bit encryption keys "offer virtually no protection at this point" from brute force attacks. "To provide adequate protection against the most serious threats... keys used to protect data today should be at least 75 bits long. To protect information adequately for the next 20 years .... keys in newly-deployed systems should be at least 90 bits long."