The latest revelation shows "an aggressive, multi-pronged effort to break widely used internet encryption. The latest revelation shows "an aggressive, multi-pronged effort to break widely used internet encryption.��� Intelligence agencies from Britain and the US have cracked many of the encryption protocols used to secure communications on the internet, according to documents leaked by the NSA whistleblower Edward Snowden. The fresh information reveals that the US National Security Agency has worked in collaboration with the the UK's GCHQ to compromise online privacy. "For the past decade, NSA has lead [sic] an aggressive, multi-pronged effort to break widely used internet encryption technologies,&#65533; reads a GCHQ document from 2010. "Vast amounts of encrypted internet data which have up till now been discarded are now exploitable." Various methods have been pursued in order to break or circumvent the security protecting the personal data of billions of people. These include breaking encryption with &#65533;brute force&#65533; attacks conducted by super computers; using court-orders to force companies into handing over master keys to their software, and one program that &#65533;actively engages US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs&#65533;. This latter scheme, named the Sigint Enabling Project, costs the NSA $254.9m a year according to a 2013 budget document provided by Snowden. Sigint stands for "signal intelligence". An internal memo from the agency records the reaction from British analysts: &#65533;Those not already briefed were gobsmacked!&#65533; &#65533;These frightening revelations imply that the NSA has not only pursued an aggressive program of obtaining private encryption keys for commercial products [&#65533;] but that the agency has also attempted to put backdoors into cryptographic standards designed to secure users' communications,&#65533; said the Electronic Frontier Foundation in response. &#65533;Additionally, the leaked documents make clear that companies have been complicit in allowing this unprecedented spying to take place, though the identities of cooperating companies remain unknown.&#65533; In response to the leaked documents - which were handed from Mr Snowden to The Guardian, The New York Times and the non-profit news site Pro Publica - Google have claimed that no such "active engagement" has taken place. "We have no evidence of any such thing ever occurring,&#65533; said the company in a statement. &#65533;We do not provide any government, including the US government, with access to our systems [&#65533;] We provide user data to governments only in accordance with the law.&#65533; The NSA described their various decryption programs as "price of admission for the US to maintain unrestricted access to and use of cyberspace&#65533;, but security experts believe that their actions are an attack against the most basic structure of the internet. &#65533;Cryptography forms the basis for trust online," Bruce Schneier, a fellow at Harvard's Berkman Center for Internet and Societ, told The Guardian. "By deliberately undermining online security in a short-sighted effort to eavesdrop, the NSA is undermining the very fabric of the internet."