The Advanced Encryption Standard (AES)

For cryptographers, a cryptographic "break" is anything faster than a brute-force attack – i.e., performing one trial decryption for each possible key in sequence.[note 7] A break can thus include results that are infeasible with current technology. Despite being impractical, theoretical breaks can sometimes provide insight into vulnerability patterns. The largest successful publicly known brute-force attack against a widely implemented block-cipher encryption algorithm was against a 64-bit RC5 key by distributed.net in 2006.[16]

The key space increases by a factor of 2 for each additional bit of key length, and if every possible value of the key is equiprobable, this translates into a doubling of the average brute-force key search time. This implies that the effort of a brute-force search increases exponentially with key length. Key length in itself does not imply security against attacks, since there are ciphers with very long keys that have been found to be vulnerable.

AES has a fairly simple algebraic framework.[17] In 2002, a theoretical attack, named the "XSL attack", was announced by Nicolas Courtois and Josef Pieprzyk, purporting to show a weakness in the AES algorithm, partially due to the low complexity of its nonlinear components.[18] Since then, other papers have shown that the attack, as originally presented, is unworkable; see XSL attack on block ciphers.

During the AES selection process, developers of competing algorithms wrote of Rijndael's algorithm "we are concerned about [its] use ... in security-critical applications."[19] In October 2000, however, at the end of the AES selection process, Bruce Schneier, a developer of the competing algorithm Twofish, wrote that while he thought successful academic attacks on Rijndael would be developed someday, he "did not believe that anyone will ever discover an attack that will allow someone to read Rijndael traffic."[20]

Until May 2009, the only successful published attacks against the full AES were side-channel attacks on some specific implementations. In 2009, a new related-key attack was discovered that exploits the simplicity of AES's key schedule and has a complexity of 2^{119}. In December 2009 it was improved to $2^{99.5}$.[2] This is a follow-up to an attack discovered earlier in 2009 by Alex Biryukov, Dmitry Khovratovich, and Ivica Nikolić, with a complexity of 2^{96} for one out of every 2^{35} keys.[21] However, related-key attacks are not of concern in any properly designed cryptographic protocol, as a properly designed protocol (i.e., implementational software) will take care not to allow related keys, essentially by constraining an attacker's means of selecting keys for relatedness.

Another attack was blogged by Bruce Schneier[22] on July 30, 2009, and released as a preprint[23] on August 3, 2009. This new attack, by Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir, is against AES-256 that uses only two related keys and 2^{39} time to recover the complete 256-bit key of a 9-round version, or 2^{45} time for a 10-round version with a stronger type of related subkey attack, or 2^{70} time for an 11-round version. 256-bit AES uses 14 rounds, so these attacks are not effective against full AES.

The practicality of these attacks with stronger related keys has been criticized,[24] for instance, by the paper on chosen-key-relations-in-the-middle attacks on AES-128 authored by Vincent Rijmen in 2010.[25]

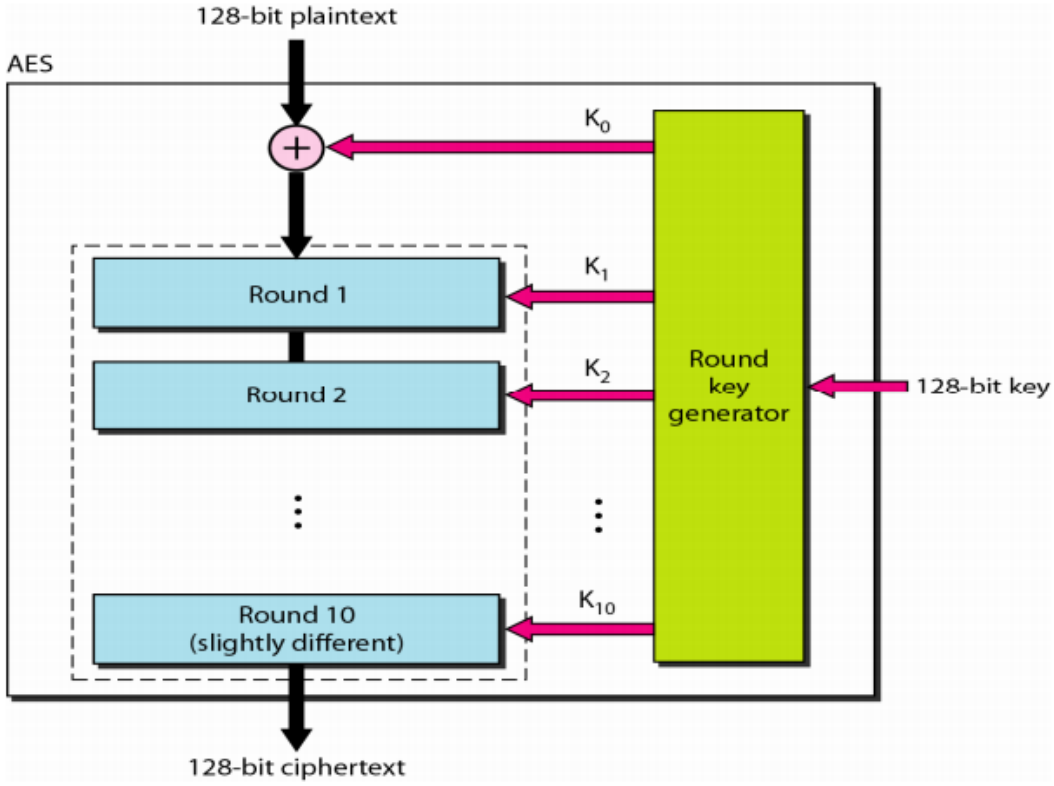

Figure 30.17 *AES*