CYBR372 - Week 3: Block Ciphers

Terms in this set (15)

What is a block cipher?	An encryption function for fixed-sized blocks of data. Block ciphers are reversible. A key is needed to encrypt and decrypt. Plaintext and ciphertext is always the same size. One rarely uses a block cipher just by itself. Use block cipher modes. Current generation of block ciphers have a block size of 128 bits. Kerchoff's Principle - Only the key should be secret, everything else including the algorithm should not be secret.

CYBR372 - Week 3: Block Ciphers

Block cipher as a key-dependent table and permutations	For any fixed key, compute a lookup table that maps plaintext to ciphertext. block cipher with: - 32-bit block size = 16GB - 64-bit block size = 150 million TB -128-bit block size = 5 * 10^39 bytes Block cipher must be reversible: No two entries of the table are the same Table will contain every possible ciphertext value at least once: Permutation Permutation - the table as a list of all possible elements where the order has been arranged. Block size k = block cipher of block size of k bits specifies a permutation on k-bit values or each of the key values. Block cipher does not permute the bits of the input plaintext. The block cipher takes all 2^k possible k-bit inputs and maps each to a unique k-bit output. eg. k = 8, input 00000001 encrypts to 01000000 with a key or 11011110 under a different key.

Secure block cipher definition and attacks	Wrong definition: A block cipher that keeps the plaintext secret (reveals nothing about the plaintext) - insufficient, requires that the block cipher be secure against ciphertext-only attacks (attacker only sees ciphertext of a message) Published attacks - Most published attacks are chosen plaintext - Related key attack - attacker has access to several encryption functions. Encryption functions have unknown keys, but there is a relationship between them. - Chosen key attack - attacker specifies some part of the key and performs a key-related attack on the rest of the key.
Ideal block cipher definition	Definition is not complete - it is an abstract concept and cannot be achieved in practice. - Should be a random permutation - one big lookup table should exist for each key value, with each table chosen randomly from the set of all possible permutations - if tables are specified, the ideal cipher is fixed and no longer random. - the ideal block cipher as a uniform probability distribution over the set of all possible block ciphers

Block cipher security definition 1 and 2	1. A secure block cipher is one for which no attack exists - quite vague, not a clear definition 2. An attack on a block cipher is a non-generic method of distinguishing the block cipher from an ideal block cipher. - distinguisher - algorithm that is given a black-box function that computes either the real block cipher or an ideal block cipher - generic and non-generic cannot be formalised - generic distinguisher - attack that can be used against any block cipher eg. generic distinguisher - encrypt 0 as plaintext with key 0 and see if result matches what we expected. advanced generic distinguisher - encrypt plaintext 0 with all keys from 1, ..., 2^32 and count the frequency of each value for the first 32 bits of the ciphertext occurs. - distinguisher as an exhaustive search of half key space = 2^n-1 and provides the right answer 75% of the time.

Permutations - distinguisher	Encryption under a key responds to a lookup in a permutation table. - permutation occurs by initialising a table by mapping element i at index i. Elements are swapped in the table. Two types of permissions - Even - most common since modern block ciphers have a 128-bit block size since they operate on 32-bit words. Encryption function is built from 32 bit operations. - Odd - very rare as it is hard to build odd permutations from small operations - virtually all block ciphers generate even permutations Parity attack distinguisher - for a given key extract the permutation by encrypting all possible plaintexts. - if odd = ideal block cipher because real block cipher never generates an off permutation. - Distinguisher will be right 75% of the time, will produce the wrong answer if the distinguisher is given an ideal block cipher that produces an even permutation. - to do this you have to compute all but one of the plaintext/ciphertext pairs of an encryption function.
Block cipher security definition 3	An ideal block cipher implements an independently chosen random even permutation for each of the key values. - definition is changed as odd parity is not feasible in practice yet. - if there exists a block cipher that can generate odd permutations, the ideal definition should be reverted to definition 2.

Real block ciphers	- Block ciphers consist of several repetitions of a weak block cipher, known as a round. - Several repetitions of weak rounds make a strong block cipher. - Most attacks begin by attacking versions with a reduced number of rounds. As attacks improve, more rounds can be attacked. - DES - AES - Serpent - Twofish - RC6 - MARS
Which block cipher should be used?	- AES - fast - 3DES for legacy systems - Double encrypt with AES then with Serpent or Twofish. Use different keys for this. - Increase rounds with AES - 16 with 128, 20 with 192, and 28 with 256. - AES, if implemented poorly, can be vulnerable to sidechannel attacks.
What key size to use?	- 128 bit security level is enough but to achieve 128 bit level security, keys longer than 128. This is due to collision attacks so we need at least 2n bits long. - hard to do this with block size since virtually all block ciphers are 128 bits. - use 256 bit keys

DES	- Deprecated - 56 bit key size - 64 bit block size - Barely surviving on 3DES - encrypt with first key, decrypt with second key, finally encrypt again with first or a third key. This fixes the small block size but does not fix the small key size. - 16 rounds - Feistel construction - Encryption and decryption is the same except that the round keys are reversed. - Weak property of using bits selected from the cipher key, if cipher key is 0, all the round keys are 0 and identical. This also provides an efficient distinguishing attack. - Has a complementation property, encrypting the complement of the plaintext with the complement of the key = complement of the original ciphertext. - 3DES may be used in legacy systems.
AES	- built with emphasis on elegance and effcientcy - Not a feistal cipher - 128 bit block cipher - support key sizes of 128 - 10 rounds, 192 - 12 rounds, and 256 - 14 rounds, bits - Achieves decent speeds as a high number of operations can be done in parallel. - Rounds can be broken theoretically with related key attacks
Serpent	- built differently, designed for maximum security - Best attack covers only 12 of 32 rounds - slow - Serpent is 1/3 of the speed of AES - utilises bitslice implementation

Twofish	- Compromise between AES and Serpent - Best attack is 8/16 rounds - Biggest disadvantage is that it can be expensive to change the encryption key - implemented with a lot of precomputation on the key - precompute s boxes - Utilises feistel structure - PHT function - Utilises whitening - start and end of cipher, additional key material is added to the data
...	...