

Symmetric cryptography

Aram Khalili

Department of Computer Science
University of Maryland

Symmetric cryptography

- Symmetric cryptography is a an outgrowth of classical cryptography.
 - All classical cryptosystem are secret key systems.
 - Most of them can be seen as block ciphers, if not, stream ciphers.
- Current symmetric cryptosystems are still secret-key system and block or stream ciphers.
- However, cryptanalytic and therefore also cryptographic techniques have significantly advanced.
- Symmetric ciphers are the fastest and therefore the most widely used cryptographic algorithms.
- They can provide confidentiality, authentication and integrity services if properly applied.

Block vs. stream ciphers

- Block ciphers break up a message into fixed size block & encrypt each one at a time. The function cannot be used until a full block of data is available.
- Stream ciphers do not work on fixed size blocks. Any amount of data can be directly encrypted. Encryption is done by generating a keystream, often independent of data. The plaintext and keystream are then combined in a mixing function. This mixing function is usually very simple, most stream ciphers use xor.
- Since the keystream can be precomputed before the data arrives, stream ciphers can be faster than block ciphers under some circumstances. However, stream ciphers, particularly with xor, have inherent weaknesses [to known-plaintext attacks].

Symmetric crypto techniques

- The basic purpose of symmetric cryptosystems is to use the key to modify the plaintext to render it unreadable/unrecognizable.
- The basic techniques for this are called confusion and diffusion.
- These roughly correspond to substitution and permutation.
- A strong cipher should contain both operations. Claude Shannon, who developed the concepts, used alternating rounds of substitution and permutation, and this design has been copied in many subsequent ciphers.

Confusion and diffusion

- Confusion is making the output dependent on the key. Ideally, every key bit influences every output bit.
- Diffusion is making the output dependent on previous input (plain/ciphertext). Ideally, each output bit is influenced by every [previous] input bit.

Avalanche and completeness effect

- Related to/measure of confusion and diffusion.
- A function has a good avalanche effect when a change in one bit of the input results in a change of half of the output bits. avalanche effect.
- A function has a good completeness effect when for each output bit i and each input bit j there exist two inputs which differ only in bit j , but whose outputs differ in bit i .

Cipher design

- symmetric ciphers need to be complex, so they can't be analyzed easily.
- also need to be simple, so they can be implemented efficiently to achieve high encryption rates.
- therefore current ciphers use simple mixing (confusion and diffusion) function, but use several rounds of them to add complexity at a small extra implementation and speed cost..

Cryptanalysis

- In addition to the traditional attacks on ciphers (known/chosen plain/ciphertext and statistical analysis), two newer forms of symmetric cryptanalysis have been developed.
- Differential cryptanalysis (a chosen plaintext attack) looks at the difference of pairs of related plaintext encrypted under same key.
- Linear cryptanalysis (a known-plaintext attack) tries to approximate the cipher successively by linear functions.

Feistel networks

- Ciphers need to be invertible, such that an encryption can be decrypted again.
- Invertible functions are easier to analyze than uninvertible functions.
- Feistel networks turn n -bit uninvertible functions into $2n$ -bit invertible functions.
- As a result the cipher is invertible, but the mixing properties of the uninvertible function still apply.

Rijndael/AES

- Designed by Vincent Rijmen and Joan Rijmen from Belgium, the name derives from their lastnames.
- The AES is the replacement for the 25 year old DES.
- Rijndael got selected as the AES in a 4-year process from call for submissions to formalization of the AES.
- There were about 30 submissions, some with design flaws that became apparent later. About twenty were seriously considered, and out of those 5 finalists were selected. All of those fulfilled the security requirements, but some had other advantages, such as speed, ease of implementation on smartcard/8- or 16-bit processors/hardware or power consumption.

Rijndael

- Block cipher with block size and key length independently varying from 128 to 256 bits in 32bit increments. AES names as block size only 128 bits and as keylength 128, 192 or 256 bits.
- Also has a variable number of rounds:
 - 10 if both the block and the key are 128 bits long.
 - 12 if either the block or the key is 192 bits long, and neither of them is longer than that.
 - 14 if either the block or the key is 256 bits long.
- An *AddRoundKey* operation precedes the first round, and the last round of each encipherment differs from the others.

AES rounds

- Each of the regular rounds has four steps. The last round for each block omits one and has only three steps.
- Rijndael/AES is not a Feistel network, all its round steps are invertible.
- For regular rounds the parts are
 - Byte substitution (ByteSub)
 - Byte permutation (ShiftRow)
 - Matrix multiplication (MixColumn)
 - Key Xor (AddRoundKey)
- The last round omits the MixColumn step.

ByteSub

- Substitutes each byte with the corresponding byte from a substitution table:

99 124 119 123 242 107 111 197 48 1 103 43 254 215 171 118 202
130 201 125 250 89 71 240 173 212 162 175 156 164 114 192 183
253 147 38 54 63 247 204 52 165 229 241 113 216 49 21 4 199 35
195 24 150 5 154 7 18 128 226 235 39 178 117 9 131 44 26 27 110
90 160 82 59 214 179 41 227 47 132 83 209 0 237 32 252 177 91 106
203 190 57 74 76 88 207 208 239 170 251 67 77 51 133 69 249 2 127
80 60 159 168 81 163 64 143 146 157 56 245 188 182 218 33 16 255
243 210 205 12 19 236 95 151 68 23 196 167 126 61 100 93 25 115
96 129 79 220 34 42 144 136 70 238 184 20 222 94 11 219 224 50 58
10 73 6 36 92 194 211 172 98 145 149 228 121 231 200 55 109 141
213 78 169 108 86 244 234 101 122 174 8 186 120 37 46 28 166 180
198 232 221 116 31 75 189 139 138 112 62 181 102 72 3 246 14 97
53 87 185 134 193 29 158 225 248 152 17 105 217 142 148 155 30
135 233 206 85 40 223 140 161 137 13 191 230 66 104 65 153 45 15
176 84 187 22

ShiftRow

- ShiftRow is a permutation of the block. If the block is 128 bits and the bytes are numbered 1-16, the permutation works as follows:

from					to				
1	5	9	13		1	5	9	13	
2	6	10	14		6	10	14	2	
3	7	11	15		11	15	3	7	
4	8	12	16		16	4	8	12	

- Other block sizes have different permutations.

MixColumn

- Multiplication by a fixed matrix.
- The block is arranged as for ShiftRow, then each column is multiplied by the matrix

$$\begin{array}{cccc} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{array}$$

- All the previous steps are diffusion steps.

AddRoundKey

- This step is an xor of the block with the key of the current round.
- The key for a round is determined by the key schedule.
- For keys 128 and 192 bits in length, the subkey material, which consists of all the round keys in order, consists of the original key, followed by stretches, each the length of the original key, consisting of four-byte words such that each word is the XOR of the preceding four-byte word and either the corresponding word in the previous stretch or a function of it. For the first word in a stretch, the word is first rotated one byte to the left, and then its bytes are transformed using the S-box from the Byte Sub step, and then a round-dependent constant is xored to its first byte.

Round constant

- Rounds range from 1-14, so the first 14 round constants are

1 2 4 8 16 32 64 128 27 54 108 216 171 77

- More are defined, but I'm not sure why.

The complete algorithm

- Initially the first round key is added (xored) to the block.
- Then $n - 1$ regular rounds are made, where n is determined by block and key size.
- A last round is made without the MixColumn step.