AES Submission Checklist

4/14/98

(Sections have been reordered for ease of review)

2.A Cover Sheet *(Barker, Foti)*

Item No.	Requirement	Included?	Initials
1	Name of submitted algorithm		
2	Principal submitter's name, phone, FAX, organization, postal address, e-mail address)		
3	Name(s) of auxiliary submitter(s)		
4	Name of algorithm inventor(s)/developer(s)		
5	Name of algorithm owner		
6	Submitter's signature		
7	(Optional) Backup point of contact (name, phone, FAX, organization, postal address, e-mail address)		
Comments:			

3. Minimum Acceptability Requirements *(Barker, Foti)*

Item No.	Requirements	Included?	Initials
8	The algorithm implements symmetric (secret) key cryptography.		
9	The algorithm is a block cipher.		
10	The algorithm supports key-block size combinations of 128-128, 192-128 and 256-128 bits as a minimum.		

Comments:

2.E General Submission Requirements *(Barker, Foti)*

Item No.	Requirements	Included?	Initials
11	Required material in the submission packages are in English – includes the cover sheet, algorithm specification, supporting documentation, source code and intellectual property information.		
12	Optional supporting materials may be provided in another language.		
13	Classified and proprietary materials not provided.		
Comments:			

2.D Intellectual Property Statements/Agreements/Disclosures (See http://csrc.nist.gov/encryption/aes/aes_9709.htm for these statements) - Must be provided in hard copy form with handwritten signature(s) and other required signature information. *(Roback)*

Item No.	Section	Requirements	Included?	Initials
14	2.D.1	Statement of the Submitter is present and complete.		
15	2.D.2	Statement by Patent (and Patent Application) Owner(s) is present and complete.		
16	2.D.3	Statement by the owner(s) of the Reference/Mathematically Optimized Implementations is present and complete.		

Comments:

2.C.5 General Requirements for Magnetic Media *(Barker, Foti)*

Item No.	Requirements	Included?	Initials
17	Separate diskettes used for the reference implementations, mathematically optimized implementations, test values and supporting materials.		
18	Magnetic media is free of viruses and other malicious code. NIST is to scan all diskettes before use.		
19	Magnetic media consists of 3.5” 1.44MB diskettes formatted for use on an IBM-compatible PC.		
20	A file labeled “README” is included on each diskette, listing and describing each file on the diskette.		
Comments:			

2.B Algorithm Specifications and Supporting Documentation *(See 2.C.4 for electronic media requirements; hard copy must be provided)*

2.B.1 Complete written algorithm specification. *(Barker, Foti)*

Item No.	Requirement	Included?	Initials
21	Hard copy and electronic versions provided (see 2.C.4 for electronic version specifications).		

Item No.	Requirement	Included?	Initials
22	Includes math. equations, tables, diagrams and parameters, as appropriate).		
23	(Optional, but encouraged) Design rationale.		
24	Bit naming/numbering convention provided.		
25	No parity bits shall be specified in the key definition.		
Comments:			

2.B.2 Statement of the algorithm's computational efficiency in hardware and software. *(Barker, Foti)*

Item No.	Requirements		Included?			Initials
26	Hard copy and electronic versions provided (see 2.C.4 for electronic version specifications).					
27	Efficiency estimates for the NIST AES analysis platform.	Platform description (see http://csrc.nist.gov/encryption/aes/aes_9709.htm).				
			128/128	**192/128**	**256/128**	
28		Speed estimates (in clock cycles) for each key/block size combination. Encrypt one data block				
29		Decrypt one data block				
30		Key setup				
31		Algorithm setup				
32		Key change				
33		(Optional) Tradeoffs between speed and memory.				

Item No.	Requirements			Included?			Initials
34	Efficiency estimates for 8-bit processors	Platform description.					
				128/128	**192/128**	**256/128**	
35		Speed estimates (in clock cycles) for each key/block size combination.	Encrypt one data block				
36			Decrypt one data block				
37			Key setup				
38			Algorithm setup				
39			Key change				
40		(Optional) Tradeoffs between speed and memory.					
41	(Optional) Efficiency estimates for other platforms.	Platform description.					
				128/128	**192/128**	**256/128**	
42		Speed estimates (in clock cycles) for each key/block size combination.	Encrypt one data block				
43			Decrypt one data block				
44			Key setup				
45			Algorithm setup				
46			Key change				
47		(Optional) Tradeoffs between speed and memory.					

Comments:

2.B.3 Known Answer tests (KATs) and Monte Carlo Tests (MCTs). *(In separate files on a diskette as described in 2.C.3; may be compressed using PKZIP or GNUZIP; see http://csrc.nist.gov/encryption/aes/ katmct/katmct.htm – Description of KATs and MCTs. A written hard copy of the tests is NOT required.) (Foti, Bassham, Dray, Barker)*

Variable Key Known Answer Test (for the encryption state) – ECB mode.. *S*ee http://csrc.nist.gov/encryption/aes/katmct/ecb_vk.txt for an example.

Item No.	Requirements		Included?	Initials
48	File name = ecb_vk.txt			
49	Keys, plaintext and ciphertext represented as ASCII hexadecimal characters. Index and key size are expressed as base 10 numbers.			
50	Correct header – filename, ECB mode, test name, algorithm name and principal submitter.			
51	Key size = 128	Key size, plaintext, index, key and ciphertext correctly labeled as specified in the example file.		
52		All zero plaintext for each encryption.		
53		128 index, key, ciphertext triples.		
54		Keys contain a single one bit and 127 zero bits.		
55		Each ciphertext decrypts to all zero plaintext.		
56	Key size = 192	Key size, plaintext, index, key and ciphertext correctly labeled as specified in the example file.		
57		All zero plaintext for each encryption.		
58		192 index, key, ciphertext triples.		
59		Keys contain a single one bit and 191 zero bits.		
60		Each ciphertext decrypts to all zero plaintext.		
61	Key size = 256	Key size, plaintext, index, key and ciphertext correctly labeled as specified in the example file.		
62		All zero plaintext for each encryption.		
63		256 index, key, ciphertext triples.		
64		Keys contain a single one bit and 255 zero bits.		
65		Each ciphertext decrypts to all zero plaintext.		
66	If applicable, other key and/or block sizes	Additional file(s) - Key size, plaintext, index, key and ciphertext correctly labeled as specified in the example file.		

Item No.	Requirements		Included?	Initials
67	(Key size = N) (Optional)	All zero plaintext for each encryption.		
68		N index, key, ciphertext triples.		
69		Keys contain a single one bit and N-1 zero bits.		
70		Each ciphertext decrypts to all zero plaintext.		
Comments:				

Variable Plaintext Known Answer Test(for the encryption state) – ECB mode. *See* http://csrc.nist.gov/encryption/aes/katmct/ecb_vt.txt for an example.

Item No.	Requirements		Included?	Initials
71	File name = ecb_vt.txt.			
72	Keys, plaintext and ciphertext represented as ASCII hexadecimal characters. Index and key size are expressed as base 10 numbers.			
73	Correct header – filename, ECB mode, test name, algorithm name and principal submitter.			
74	Key size = 128	Key size, key, index, plaintext and ciphertext correctly labeled as specified in the example file.		
75		All zero key for each encryption.		
76		128 index, plaintext, ciphertext triples.		
77		Plaintext contains a single one bit and 127 zero bits.		
78		Each ciphertext decrypts to the original plaintext.		
79	Key size = 192	Key size, key, index, plaintext and ciphertext correctly labeled as specified in the example file.		
80		All zero key for each encryption.		

Item No.	Requirements		Included?	Initials
81		128 index, plaintext, ciphertext triples.		
82		Plaintext contains a single one bit and 127 zero bits.		
83		Each ciphertext decrypts to the original plaintext.		
84	Key size = 256	Key size, key, index, plaintext and ciphertext correctly labeled as specified in the example file.		
85		All zero key for each encryption.		
86		128 index, plaintext, ciphertext triples.		
87		Plaintext contains a single one bit and 127 zero bits.		
88		Each ciphertext decrypts to the original plaintext.		
89	If applicable, other key and/or block sizes	Additional file(s) - Key size, key, index, plaintext and ciphertext correctly labeled as specified in the example file.		
90	(Key size = N)	All zero key for each encryption.		
91	(Optional)	128 index, plaintext, ciphertext triples.		
92		Plaintext contains a single one bit and 127 zero bits.		
93		Each ciphertext decrypts to the original plaintext.		
Comments:				

Intermediate Values Known Answer Test (If applicable) – Encryption and Decryption

Item No.	Requirements	Included?	Initials
94	File name = [IDENTIFY]		
95	Description of what is being tested.		

Item No.	Requirements		Included?	Initials
96	Keys, plaintext, intermediate values and ciphertext represented as ASCII hexadecimal characters. Index and key size are expressed as base 10 numbers.			
97	Precise description of how and where testing is performed in the algorithm.			
98	Correct header – filename, ECB mode, test name, algorithm name and principal submitter.			
99	Key size = 128	Key size, key, index, plaintext, intermediate values and ciphertext correctly labeled.		
100		Key, plaintext and ciphertext specified.		
101		Index and intermediate value pairs as appropriate for one encryption.		
102		Index and intermediate value pairs as appropriate for one decryption back to the original plaintext.		
103	Key size = 192	Key size, key, index, plaintext, intermediate values and ciphertext correctly labeled.		
104		Key, plaintext and ciphertext specified.		
105		Index and intermediate value pairs as appropriate for one encryption.		
106		Index and intermediate value pairs as appropriate for one decryption back to the original plaintext.		
107	Key size = 256	Key size, key, index, plaintext, intermediate values and ciphertext correctly labeled.		
108		Key, plaintext and ciphertext specified.		
109		Index and intermediate value pairs as appropriate for one encryption.		
110		Index and intermediate value pairs as appropriate for one decryption back to the original plaintext.		
111	If applicable, other key and/or block sizes (Key size = N) (Optional)	Key size, key, index, plaintext, intermediate values and ciphertext correctly labeled.		
112		Key, plaintext and ciphertext specified.		
113		Index and intermediate value pairs as appropriate for one encryption.		
114		Index and intermediate value pairs as appropriate for one decryption back to the original plaintext.		
Comments:				

Tables Known Answer Test (if applicable)– ECB Mode. *See* http://csrc.nist.gov/encryption/aes/katmct/ecb_tbl.txt for an example.

Item No.	Requirements		Included?	Initials
115	File name = ecb_tbl.txt.			
116	Keys, plaintext and ciphertext represented as ASCII hexadecimal characters. Index and key size are expressed as base 10 numbers.			
117	Correct header – filename, ECB mode, test name, algorithm name and principal submitter. Include a description of what tables are tested (see example file specified above).			
118	Key size = 128	Key size, key, index, plaintext and ciphertext correctly labeled as specified in the example file for an encryption.		
119		Index, key, plaintext, ciphertext sets. The number of sets is algorithm dependent.		
120		Each ciphertext decrypts to the original plaintext.		
121	Key size = 192	Key size, key, index, plaintext and ciphertext correctly labeled as specified in the example file for an encryption.		
122		Index, key, plaintext, ciphertext sets. The number of sets is algorithm dependent.		
123		Each ciphertext decrypts to the original plaintext.		
124	Key size = 256	Key size, key, index, plaintext and ciphertext correctly labeled as specified in the example file for an encryption.		
125		Index, key, plaintext, ciphertext sets. The number of sets is algorithm dependent.		
126		Each ciphertext decrypts to the original plaintext.		
127	If applicable, other key and/or block sizes	Additional file(s) - Key size, key, index, plaintext and ciphertext correctly labeled as specified in the example file for an encryption.		
128	(Key size = N)	Index, key, plaintext, ciphertext sets. The number of sets is algorithm dependent		
129	(Optional)	Each ciphertext decrypts to the original plaintext.		
Comments:				

ECB Encrypt Monte Carlo Tests. *See* http://csrc.nist.gov/encryption/aes/katmct/ecb_e_m.txt for an example.

Item No.	Requirements		Included?	Initials
130	Filename = ecb_e_m.txt			
131	Keys, plaintext and ciphertext represented as ASCII hexadecimal characters. Index and key size are expressed as base 10 numbers.			
132	Correct header – filename, ECB mode, test name, algorithm name and principal submitter.			
133	Key size = 128	Key size, index, key, plaintext and ciphertext correctly labeled as specified in the example file.		
134		400 sets of index, key, plaintext, and ciphertext are present.		
135	Key size = 192	Key size, index, key, plaintext and ciphertext correctly labeled as specified in the example file.		
136		400 sets of index, key, plaintext, and ciphertext are present.		
137	Key size = 256	Key size, index, key, plaintext and ciphertext correctly labeled as specified in the example file.		
138		400 sets of index, key, plaintext, and ciphertext are present.		
139	If applicable, other key and/or block sizes (Optional)	Additional file(s) - Key size, index, key, plaintext and ciphertext correctly labeled as specified in the example file.		
140		400 sets of index, key, plaintext, and ciphertext are present.		
Comments:				

ECB Decrypt Monte Carlo Tests. *See* http://csrc.nist.gov/encryption/aes/katmct/ecb_d_m.txt for an example.

Item No.	Requirements		Included?	Initials
141	Filename = ecb_d_m.txt			
142	Keys, plaintext and ciphertext represented as ASCII hexadecimal characters. Index and key size are expressed as base 10 numbers.			
143	Correct header – filename, ECB mode, test name, algorithm name and principal submitter.			
144	Key size = 128	Key size, index, key, ciphertext and plaintext correctly labeled as specified in the example file.		
145		400 sets of index, key, ciphertext, and plaintext are present.		
146	Key size = 192	Key size, index, key, ciphertext and plaintext correctly labeled as specified in the example file.		
147		400 sets of index, key, ciphertext, and plaintext are present.		
148	Key size = 256	Key size, index, key, ciphertext and plaintext correctly labeled as specified in the example file.		
149		400 sets of index, key, ciphertext, and plaintext are present.		
150	If applicable, other key and/or block sizes (Optional)	Additional file(s) - Key size, index, key, ciphertext and plaintext correctly labeled as specified in the example file.		
151		400 sets of index, key, ciphertext, and plaintext are present.		
Comments:				

CBC Encrypt Monte Carlo Tests. *See* http://csrc.nist.gov/encryption/aes/katmct/cbc_e_m.txt for an example.

Item No.	Requirements		Included?	Initials
152	Filename = cbc_e_m.txt			
153	Keys, IV, plaintext and ciphertext represented as ASCII hexadecimal characters. Index and key size are expressed as base 10 numbers.			
154	Correct header – filename, CBC mode, test name, algorithm name and principal submitter.			
155	Key size = 128	Key size, index, key, IV, plaintext and ciphertext correctly labeled as specified in the example file.		
156		400 sets of index, key, IV, plaintext, and ciphertext are present.		
157	Key size = 192	Key size, index, key, IV, plaintext and ciphertext correctly labeled as specified in the example file.		
158		400 sets of index, key, IV, plaintext, and ciphertext are present.		
159	Key size = 256	Key size, index, key, IV, plaintext and ciphertext correctly labeled as specified in the example file.		
160		400 sets of index, key, IV, plaintext, and ciphertext are present.		
161	If applicable, other key and/or block sizes (Optional)	Additional file(s) - Key size, index, key, IV, plaintext and ciphertext correctly labeled as specified in the example file.		
162		400 sets of index, key, IV, plaintext, and ciphertext are present.		
Comments:				

CBC Decrypt Monte Carlo Tests. *See* http://csrc.nist.gov/encryption/aes/katmct/cbc_d_m.txt for an example.

Item No.	Requirements		Included?	Initials
163	Filename = cbc_d_m.txt			
164	Keys, IV, ciphertext and plaintext represented as ASCII hexadecimal characters. Index and key size are expressed as base 10 numbers.			
165	Correct header – filename, CBC mode, test name, algorithm name and principal submitter.			
166	Key size = 128	Key size, index, key, IV, ciphertext and plaintext correctly labeled as specified in the example file.		
167		400 sets of index, key, IV, ciphertext, and plaintext are present.		
168	Key size = 192	Key size, index, key, IV, ciphertext and plaintext correctly labeled as specified in the example file.		
169		400 sets of index, key, IV, ciphertext, and plaintext are present.		
170	Key size = 256	Key size, index, key, IV, ciphertext and plaintext correctly labeled as specified in the example file.		
171		400 sets of index, key, IV, ciphertext, and plaintext are present.		
172	If applicable, other key and/or block sizes.	Additional file(s) - Key size, index, key, IV, ciphertext and plaintext correctly labeled as specified in the example file.		
173	(Optional)	400 sets of index, key, IV, ciphertext, and plaintext are present.		
Comments:				

2.B.4 Statement of Expected Strength (i.e., work factor) *(Barker, Foti)*

Item No.	Requirements		Included?	Initials
174	Hard copy and electronic versions required (see 2.C.4 for electronic version specifications).			
175	Key size = 128	Expected strength.		
176	Block size = 128	Supporting rationale.		
177	Key size = 192	Expected strength.		
178	Block size = 128	Supporting rationale.		
179	Key size = 256	Expected strength.		
180	Block size = 128	Supporting rationale.		
181	Other key size & block size combinations (Required, if applicable)	Expected strength.		
182		Supporting rationale.		
Comments:				

2.B.5 Algorithm Analysis *(Barker, Foti)*

Item No.	Requirements	Included?	Initials
183	Hard copy and electronic versions required (see 2.C.4 for electronic version specifications).		
184	Analysis of the algorithm with respect to known attacks		
185	Statement regarding known weak keys, equivalent keys complementation properties, restrictions on key selection and other similar features. Must be addressed even if these values are unknown.		
186	Statement regarding any mathematical rationale for the non-existence of “trap doors”.		
187	List of known references to published materials describing or analyzing the security of the algorithm.		

Item No.	Requirements	Included?	Initials
188	(Optional, but encouraged) Copies of published materials plus copyright waiver or permission from the copyright holder for AES public evaluation purposes.		
Comments:			

2.B.6 Algorithm Advantages and Limitations *(Barker, Foti)*

Item No.	Requirements	Included?	Initials
189	Hard copy and electronic versions required (see 2.C.4 for electronic version specifications).		
190	General statement that lists and describes the advantages and limitations of the algorithm.		
191	Statement of the ability to implement the algorithm as a stream cipher, MAC generator, pseudo-random number generator, hashing algorithm, etc. Each must be addressed even if the advantages/liabilities are unknown.		
192	Statement of the ability to implement the algorithm in various environments, including 8-bit processors (smart cards), ATM, HDTV, B-ISDN, voice applications, satellite applications, etc. Each must be addressed even if the advantages/liabilities are unknown.		
193	(Optional) Specification of the algorithm in a non-proprietary Hardware Description Language (HDL).		
194	Statement of the ability to use the algorithm with key and block sizes other than the required combinations.		
195	(Optional) Other advantageous features of the algorithm -- listed and described along with supporting rationale.		

Item No.	Requirements	Included?	Initials
Comments:			

2.C Magnetic Media

2.C.1 Reference Implementation *(Bassham)*

Item No.	Requirements	Included?	Initials
196	ANSI C source code (reference implementation) uses NIST-specified API. (either new version or 4/6/98 version)	API used:	
197	Code contains appropriate comments.		
198	Comments map to the algorithm description in 2.B.1.		
199	Supports a key size of 128 and block size of 128.		
200	Supports a key size of 192 and block size of 128.		
201	Supports a key size of 256 and block size of 128.		
202	Supports all other key sizes and block sizes which have been claimed in 2.B.6 (Required).		
203	ANSI C source code for implementing the Known Answer tests for the reference implementation.		
204	ANSI C source code for implementing the Monte Carlo tests for the reference implementation.		
205	Source code for exercising the KATs and MCTs outputs data in formats specified in 2.B.3. *(Run software and verify that correct output values are generated.)*		
206	Code for the ANSI C reference implementation, KATs, and MCTs provided on a single diskette, labeled with the submitter's name, algorithm name and "Reference Implementation". For preliminary submissions, there may be a separate disk marked "Reference Implementation – KATs and MCTs" for the KAT/MCT source code. Both the reference implementation and KAT/MCT source code should eventually be placed on the "Reference Implementation" disk for the final submission.		

Item No.	Requirements	Included?	Initials
207	(Optional) Instructions for interfacing the reference implementation.		
208	Instructions for running the Known Answer Test and Monte Carlo Tests.		
Comments:			

2.C.2 Mathematically Optimized Implementations (See http://csrc.nist.gov/encryption/aes/aes_9709.htm) *(Bassham, Dray)*

Item No.	Requirements		Included?	Initials
210	ANSI C	Optimized implementation provided in ANSI C source code.		
211	*Bassham*	Uses NIST-specified API. (either new version or 4/6/98 version)	API used:	
212		Includes comments and clarifications of changes (see API example).		
213		Supports key size = 128, block size = 128.		
214		Supports key size = 192, block size = 128.		
215		Supports key size = 256, block size = 128.		
216		(Optional) Supports other key and block sizes specified in 2.B.6.		
217		Supports ECB mode for encryption and decryption.		
218		Supports CBC mode for encryption and decryption.		
219		Supports 1-bit CFB mode for encryption and decryption.		
220		Source code for exercising Known Answer Tests (KATs) and Monte Carlo Tests (MCTs) for the ANSI C optimized implementation. (not required for Intermediate Values KATs) **(Run software and verify that correct output values are generated.)*		
221		Code for the ANSI C optimized implementation, KATs and MCTs supplied on a diskette labeled with the submitter's name, algorithm name and "Optimized ANSI C".		

Item No.	Requirements		Included?	Initials
222	Java	Optimized implementation provided in Java source code		
223	*Dray*	Uses cryptographic API defined by NIST/Cryptix new Java API spec as specified in http://csrc.nist.gov/encryption/aes/api/api.htm.; may use either the Java Cryptography Architecture (JCA) and the Java Cryptography Extension (JCE) – version 1.2 – or IJCE 1.1 for preliminary submissions.	API used:	
224		(If using JCE or IJCE API) Cryptography Package Provider (CPP) supplied which implements the algorithm. The provider package name must follow the naming conventions specified in the Cryptographic API Profile. ***(Evaluator- make sure this is entered on the checklist cover sheet.)***		
225		Supports key size = 128, block size = 128.		
226		Supports key size = 192, block size = 128.		
227		Supports key size = 256, block size = 128.		
228		(Optional) Supports other key and block sizes specified in 2.B.6.		
229		Supports ECB mode for encryption and decryption.		
230		Supports CBC mode for encryption and decryption.		
231		Supports 1-bit CFB mode for encryption and decryption.		
232		Source code for exercising Known Answer Tests and Monte Carlo Tests for the Java optimized implementation. (not required for Intermediate Values KATs) **(Run software and verify that correct output values are generated.)*		
233		Code for the Java optimized implementation, KATs and MCTs supplied on a diskette labeled with the submitter's name, algorithm name and "Optimized Java".		

Comments:

2.C.3 Test Values – Known Answer Tests and Monte Carlo Tests *(Bassham, Dray)*

Item No.	Requirements	Included?	Initials
234	KAT and MCT test values from 2.B.3 on a single diskette.		
235	(Optional) May be compressed using PKZIP or GNUZIP.		
236	Diskette is labeled with submitter's name, algorithm name and "Test Values: Known Answer Tests and Monte Carlo Tests".		
Comments:			

2.C.4 Supporting Documentation *(Barker, Foti)*

Item No.	Requirements	Included?	Initials
237	All written (hard copy) materials must also be submitted in Postscript or Adobe PDF. PDF is preferable.		
238	PDF files (if used) use thumbnail and bookmark features and a clickable table of contents (optional, but encouraged).		
239	Postscript files (if used) use standard Postscript printer fonts.		
240	Materials provided on diskette(s) labeled with the submitter's name, algorithm name and "Supporting Documentation".		
241	If multiple diskettes are used, include "*#m of n*" on the label, where *n* is the number of diskettes, and *1£m£n*.		
Comments:			