ID²固定密钥验证

Rev 1.0

Release Date: 2018-04-28

1.概述

1.1 目的

本文档定义了几组固定密钥，用于调试阶段的正确性验证。

备注：该文档所描述密钥仅用于调试阶段的正确性验证，不能用于正式产品!!!

2. 3DES 固定密钥

2.1 CONST_3DES_112

ID2: 0102030405060708090A0B0C
KEY: 0102030405060708090A0B0C0D0E0F10

2.2 CONST_3DES_168

ID2: 1112131415161718191A1B1C
KEY: 1112131415161718191A1B1C1D1E1F202122232425262728

3. AES 固定密钥

3.1 CONST_AES_128

ID2: 2122232425262728292A2B2C
KEY: 2122232425262728292A2B2C2D2E2F30

3.2 CONST_AES_192

ID2: 3132333435363738393A3B3C
KEY: 3132333435363738393A3B3C3D3E3F404142434445464748

3.3 CONST_AES_256

ID2: 4142434445464748494A4B4C
KEY: 4142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F60

4. RSA 固定密钥

4.1 CONST_RSA_1024

ID2: 5152535455565758595A5B5C
N:
E3 B6 89 5C 2F 01 D4 A7 7A 4D 1F F2 C5 98 6B 3E
10 E3 B6 89 5C 2F 01 D4 A7 7A 4D 1F F2 C5 98 6B
3E 10 E3 B6 89 5C 2F 01 D4 A7 7A 4D 1F F2 C5 98
6B 3E 10 E3 B6 89 5C 2F 01 D4 A7 7A 4D 1F F1 F3
59 86 B3 E1 0E 3B 68 95 C2 F0 1D 4A 77 A4 D1 FF
2C 59 86 B3 E1 0E 3B 68 95 C2 F0 1D 4A 77 A4 D1
FF 2C 59 86 B3 E1 0E 3B 68 95 C2 F0 1D 4A 77 A4
D1 FF 2C 59 86 B3 E1 0E 3B 68 95 C2 F0 1D 7A B3
E:
01 00 01
D:
A5 AE 76 9B 00 08 D0 F5 5A 63 2B 4F B4 BD 85 AA
0F 17 E0 04 69 72 3A 5E C3 CC 94 B9 1E 26 EF 13
78 81 49 6D D2 DB A3 C8 2D 35 FE 22 87 90 58 7C
E1 EA B2 D7 3C 45 0D 31 96 9F 67 8B F0 F9 C1 4B
F3 0A 96 51 98 B0 3B F7 3E 55 E1 9C E3 FB 87 42
89 A1 2C E8 2F 46 D2 8D D4 EC 78 33 7A 92 1D D9
20 37 C3 7E C5 DD 69 24 6B 83 0E CA 11 28 B4 6F
B6 CE 5A 15 5C 73 FF BB 02 19 A5 60 A7 BF 6E C1

P:

F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0

F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0

F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0

F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 F0 79

Q:

F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1

F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1

F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1

F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 F1 8B

DP:

0E 0E 10 10 0E 0E 10 10 0E 0E 10 10 0E 0E 10 10

0E 0E 10 10 0E 0E 10 10 0E 0E 10 10 0E 0E 10 10

0E 0E 10 10 0E 0E 10 10 0E 0E 10 10 0E 0E 10 10

0E 0E 10 10 0E 0E 10 10 0E 0E 10 10 0E 0E 10 09

DQ:

A6 C7 18 F8 A6 C7 18 F8 A6 C7 18 F8 A6 C7 18 F8

A6 C7 18 F8 A6 C7 18 F8 A6 C7 18 F8 A6 C7 18 F8

A6 C7 18 F8 A6 C7 18 F8 A6 C7 18 F8 A6 C7 18 F8

A6 C7 18 F8 A6 C7 18 F8 A6 C7 18 F8 A6 C7 18 B1

QINV:

3E 33 59 35 7B 78 E9 65 47 C5 BA E0 BD 03 00 70

EC CF 4D 42 68 44 8A 87 F8 74 56 D4 C9 EF CC 12

0F 7F FB DE 5C 51 77 53 99 97 07 83 65 E3 D8 FE

DB 21 1E 8F 0A ED 6B 60 86 62 A8 A6 16 92 74 D4

5. 正确性验证

5.1 挑战字方式

示例 Demo 中，请使用如下固定参数：

challenge： "55B83408399FA660F05C82E4F25333DC"

without extra： NULL

with extra： "abcd1234"

5.2 时间戳方式

示例 Demo 中，请使用如下固定参数：
timestamp： "1512022279204"
without extra： NULL
with extra： "abcd1234"

5.3 设备端随机数

irot_pal_get_random 在调试验证阶段，请返回 0xAB, 0xAB, 0xAB, 0xAB ……，用于临时验证。临时验证完毕，请返回真随机数，以用于正式产品！！！

5.4 认证码 (SHA-256 哈希算法)

5.4.1 CONST_3DES_112

[110]
0~2~ABABABABABABABAB~55B83408399FA660F05C82E4F25333DC~70J2tJTgCuxw+Z0+ZobpI+KeqIk60LJ392ir3mb/bxQGEBk3fGv9ig==
[110]
2~2~ABABABABABABABAB~55B83408399FA660F05C82E4F25333DC~ZIiaRKufjGz6cE0K+CAN8FMTzlCqJer38PpLGJOWvyMGEBk3fGv9ig==
[91]
1~2~ABABABABABABABAB~1512022279204~jc4s3XsfCohoDdOZLefossf/JQ0NTDgjJGKIROZWNCwGEBk3fGv9ig==
[91]
3~2~ABABABABABABABAB~1512022279204~ALUsRGY99COJsC5DAGTn0EXvNu8nLLM8mpjCuGkVEasGEBk3fGv9ig==

5.4.2 CONST_3DES_168

[110]
0~2~ABABABABABABABAB~55B83408399FA660F05C82E4F25333DC~uJj86Mwq2mOxtN6talgMM4RrE70lEWpN4UvtzjK5lv96EILhmqwRyQ==
[110]
2~2~ABABABABABABABAB~55B83408399FA660F05C82E4F25333DC~ghXSTRrL3U5YN6ri/8UfCaHuP6SWUNK/qGm4JkvQ1/Z6EILhmqwRyQ==
[91]
1~2~ABABABABABABABAB~1512022279204~RR7e0wQMTvOlfUo4tq0Le23JC1VOSxPrJqmNFCVK+Zt6EILhmqwRyQ==
[91]
3~2~ABABABABABABABAB~1512022279204~Ho0RdKQevV1O4pf/sjaYjkaytD8WSkHNR3rNS/+UQ7h6EILhmqwRyQ==

5.4.3 CONST_AES_128

[118]
0~2~ABABABABABABABAB~55B83408399FA660F05C82E4F25333DC~4sx4q/vZtJeBciBhpfzBwLaw7kXg4s2mmZxSoehsKtyXnA1nt3r97vPi1Bnh6fF1
[118]
2~2~ABABABABABABABAB~55B83408399FA660F05C82E4F25333DC~PdEkTetZVHtD3+o64apuEnsgzwkqbJMfTJSMaHTSYFKXnA1nt3r97vPi1Bnh6fF1
[99]
1~2~ABABABABABABABAB~1512022279204~8WFAQalYm+5++M4OKMtH2JOqsvOlS67rsX9ccSRpvWSXnA1nt3r97vPi1Bnh6fF1
[99]
3~2~ABABABABABABABAB~1512022279204~3vxizdS0JVOKSqnsR8VsZd0xUnL7Uo2S4ojSgXnoxI6XnA1nt3r97vPi1Bnh6fF1

5.4.4 CONST_AES_192

[118]
0~2~ABABABABABABABAB~55B83408399FA660F05C82E4F25333DC~l9OCInShWFDSu
WM0CoiMUBo91GIiEuBUJS9geca8UznOa4mLlgC4KH2vzjV50c24
[118]
2~2~ABABABABABABABAB~55B83408399FA660F05C82E4F25333DC~KrMAH6EK8Xz+
ATR/55dj5+NdLwsdP4ixY0qv9P+eUDTOa4mLlgC4KH2vzjV50c24
[99]
1~2~ABABABABABABABAB~1512022279204~hZhuHqK46xCV8EOwTct021/C/HphULzRu2
xUF2d8rrfOa4mLlgC4KH2vzjV50c24
[99]
3~2~ABABABABABABABAB~1512022279204~1g3tbvrsZVuAireQWhDNJLhO/dfllMpZvp6F
PqJDSrnOa4mLlgC4KH2vzjV50c24

5.4.5 CONST_AES_256

[118]
0~2~ABABABABABABABAB~55B83408399FA660F05C82E4F25333DC~Go3Am1MyVbya4
wIeWr61K23iIp5r104lYFtWCx45MB5msyC++8NwDRew+8a7MqUo
[118]
2~2~ABABABABABABABAB~55B83408399FA660F05C82E4F25333DC~FMQCgFHZ+zcV+
I752yS4QNmpb8sqwi7EFpsRbDBUnSJmsyC++8NwDRew+8a7MqUo
[99]
1~2~ABABABABABABABAB~1512022279204~JSNDoKjn7psgDyoiBBUhNY6l4H3O7xadnD
xoUd6AhdlmsyC++8NwDRew+8a7MqUo
[99]
3~2~ABABABABABABABAB~1512022279204~13zePuxAvpnt37Jx88Nt17rqN8HCGdyrkwB
GAAp8vR5msyC++8NwDRew+8a7MqUo

5.5 解密（id2_client_decrypt)

示例 Demo 中，请使用如下固定参数：
明文数据(4 字节)："1234"
密文数据根据密钥类型和长度不同，分别使用如下数据：

5.5.1 CONST_3DES_112

0xA0, 0xFA, 0x13, 0x44, 0x96, 0x0D, 0x4E, 0xBA

5.5.2 CONST_3DES_168

0x84, 0xAC, 0xA5, 0x93, 0x71, 0xAE, 0x5F, 0x36

5.5.3 CONST_AES_128

0xEC, 0xE1, 0x8C, 0xE9, 0xB9, 0x61, 0xAE, 0xD7,
0x50, 0x02, 0xA4, 0x8E, 0xB9, 0x95, 0x5E, 0x44

5.5.4 CONST_AES_192

0x8D, 0x07, 0xF6, 0x38, 0x52, 0x28, 0x25, 0xBD,
0x28, 0xD3, 0x1D, 0x8D, 0xCA, 0x21, 0xB6, 0xE9

5.5.5 CONST_AES_256

0x72, 0x8D, 0x1F, 0xDB, 0x02, 0x3B, 0x7D, 0x37,
0xAA, 0x47, 0xDA, 0x0F, 0x19, 0x6A, 0x37, 0x13