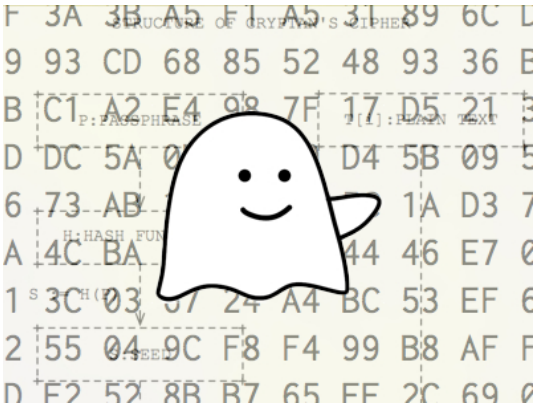
暗号解読クリプタン問題

http://www.hyuki.com/codeiq/

2014 年 3 月



1　概要

あなたはクリプタン帝国にプログラマとして雇われました。あなたは、依頼に基づき「暗号文」二つを解読しなければなりません。それぞれの「暗号文」にはクリプタン帝国の諜報員が入手した「暗号プログラムの構成図」が付随していますが、十分な情報はありません。「暗号文」二つを解読して、暗号化する前の文章を復元することがあなたのミッションなのです！

2　会話

あなた「暗号文を解読する仕事と聞きましたが、いったいどういうことでしょうか……」

依頼者「順を追って説明しましょう。わがクリプタン帝国では厳しい情報規制が行われており、一般国民は暗号プログラムを使うことがゆるされていません。しかし最近、一部の《不穏分子》が暗号プログラムを使った通信を行っているようなのです。わが国の諜報員はその「暗号文」を二つ入手し、さらにはそれぞれの暗号化に使われた「暗号プログラムの構成図」も入手しました」

あなた「は、はあ、そうなんですか。ふ、不穏分子が……」

依頼者「そこであなたにはその暗号文を暗号解読して、暗号化する前の文章を復元していただきたい」

あなた「そういうことなのですね。ちなみに、文章が復元できた場合、その《不穏分子》とやらはどのような扱いを受けるのでしょうか……」

依頼者「それは文章の内容によります。そう思いませんか？　もしもわが帝国の安全を揺るがす内容ならば、それ相応の処罰をせねばなりますまい（キリッ）」

あなた「それは……そう、なのかもしれません、けれど」

依頼者「ともかく、あなたのお仕事は暗号解読です」

あなた「わかりました。それではその「暗号文」と「暗号プログラムの構成図」を見せていただけますか」

依頼者「その前に注意点が一つ。「暗号プログラムの構成図」はあくまで構成図であって、詳細まで書かれているわけではありません。概略図とヒントだと思っていただいた方がいいでしょう。そもそもこの「暗号プログラムの構成図」を入手するのだけでもたいへんだったのです」

あなた「なるほど」

依頼者「あなたは優秀なプログラマでいらっしゃるから、不明点は推測することができるだろうと期待しています」

あなた「努力します」

暗号文 1

依頼者「それではまず一つ目の暗号文です（図 1 cryptan1.txt）。ここでは暗号文を 16 進表示していますが、暗号前の文章は **ASCII** コードで書かれたことがわかっています」

```
78 AB DA 58 CB 0D 9C 9C 21 CB E4 2C CB 7D 9C F0
1C CB CE F0 BA 0D DA 24 21 78 CB 25 25 CB 4D 9C
CB 3F 1C DA 3F 3F 9C 7D CB 4D C2 0D CB BA 9C 0D
BA 25 BA 58 D3 9C CB C2 24 CB BA 4D 9C CB 1C F0
CD A9 21 CB F0 24 7D CB D3 9C 08 F0 24 CB BA DA
CB 97 9C CD BA 58 1C 9C CB 07 C2 BA 4D CB BA 4D
9C CB F0 C2 1C CB DA F9 CB F0 CB 3F 1C DA F9 9C
0D 0D DA 1C CB F0 7D 7D 1C 9C 0D 0D C2 24 08 CB
4D C2 0D CB CD 97 F0 0D 0D CB 25 25 CB 78 C2 BA
CB C2 0D CB 24 DA BA CB 1C 9C F0 97 97 2C CB 7D
C2 F9 F9 C2 CD 58 97 BA CB BA DA CB CD DA 24 0D
BA 1C 58 CD BA CB F0 CB 0D 9C 1C C2 9C 0D CB DA
F9 CB C2 24 F9 9C 1C 9C 24 CD 9C 0D 21 CB 9C F0
CD 4D CB 7D 9C 3F 9C 24 7D 9C 24 BA CB 58 3F DA
24 CB C2 BA 0D CB 3F 1C 9C 7D 9C CD 9C 0D 0D DA
1C CB F0 24 7D CB 9C F0 CD 4D CB 0D C2 E4 3F 97
9C CB C2 24 CB C2 BA 0D 9C 97 F9 50 CB CB B7 F9
21 CB F0 F9 BA 9C 1C CB 7D DA C2 24 08 CB 0D DA
21 CB DA 24 9C CB 0D C2 E4 3F 97 2C CB A9 24 DA
CD A9 0D CB DA 58 BA CB F0 97 97 CB BA 4D 9C CB
CD 9C 24 BA 1C F0 97 CB C2 24 F9 9C 1C 9C 24 CD
9C 0D CB F0 24 7D CB 3F 1C 9C 0D 9C 24 BA 0D CB
DA 24 9C C5 0D CB F0 58 7D C2 9C 24 CD 9C CB 07
C2 BA 4D CB BA 4D 9C CB 0D BA F0 1C BA C2 24 08
25 3F DA C2 24 BA CB F0 24 7D CB BA 4D 9C CB CD
DA 24 CD 97 58 0D C2 DA 24 21 CB DA 24 9C CB E4
F0 2C CB 3F 1C DA 7D 58 CD 9C CB F0 CB 0D BA F0
1C BA 97 C2 24 08 21 CB BA 4D DA 58 08 4D CB 3F
DA 0D 0D C2 D3 97 2C CB F0 CB E4 9C 1C 9C BA 1C
C2 CD C2 DA 58 0D 21 CB 9C F9 F9 9C CD BA 50 CB
88 DA 07 21 CB C2 BA CB 07 F0 0D CB 24 DA BA CB
1C 9C F0 97 97 2C CB 7D C2 F9 F9 C2 CD 58 97 BA
21 CB D3 2C CB F0 24 CB C2 24 0D 3F 9C CD BA C2
DA 24 CB DA F9 CB BA 4D 9C CB 08 1C DA DA 7F 9C
CB D3 9C BA 07 9C 9C 24 CB 2C DA 58 1C CB 97 9C
F9 BA CB F9 DA 1C 9C F9 C2 24 08 9C 1C CB F0 24
7D CB BA 4D 58 E4 D3 21 CB BA DA CB F9 9C 9C 97
CB 0D 58 1C 9C CB BA 4D F0 BA CB 2C DA 58 CB 7D
C2 7D CB 88 AC 9D CB 3F 1C DA 3F DA 0D 9C CB BA
DA CB C2 24 7F 9C 0D BA CB 2C DA 58 1C CB 0D E4
F0 97 97 CB CD F0 3F C2 BA F0 97 CB C2 24 CB BA
4D 9C CB 08 DA 97 7D CB F9 C2 9C 97 7D 0D 50 78
```

図 1　暗号文 1 を 16 進表示したもの（cryptan1.txt）

あなた「なるほど」

依頼者「この cryptan1.txt は後ほどテキストファイルとしてお渡しします」

あなた「助かります」

依頼者「そしてこの暗号文 1 を作り出した暗号プログラムの構成図 1 がこちらです（図 2)」

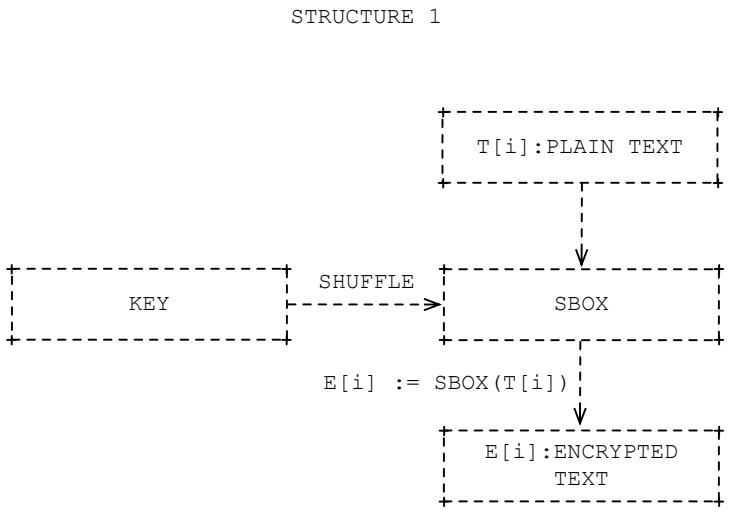


図 2　暗号プログラムの構成図 1

あなた「これは……確かに概略ですね」

暗号文 2

依頼者「二つ目の暗号文がこれです（図 3 cryptan2.txt）。こちらも暗号文を 16 進表示していますが、暗号前の文章は **ASCII** コードで書かれたことがわかっています」

```
C8 EE A8 0F 80 FD 60 E9 00 3F C4 B0 10 2C E7 33
DC 82 1E 6B D3 5B BB FA 8A 48 C2 F0 97 7F A6 C0
9C 32 15 89 37 51 AA C9 D8 93 9D 86 DA 28 BB 58
A2 6D E2 7F 3A 3B A5 F1 A5 31 89 6C D8 B5 E6 15
BC A4 BC 59 93 CD 68 85 52 48 93 36 B1 F4 5E FA
D1 62 7C 4B C1 A2 E4 98 7F 17 D5 21 37 7F C5 A0
2C BE 67 4D DC 5A 0B 66 D9 D4 5B 09 58 2F 72 ED
4F 45 81 36 73 AB 18 DF 51 5C 1A D3 7F 2E EF B8
D8 C8 C0 8A 4C BA 87 23 01 44 46 E7 03 42 EF 44
EA 05 36 11 3C 03 67 24 A4 BC 53 EF 6E 2D C3 66
B9 CF 9C C2 55 04 9C F8 F4 99 B8 AF FF EA 16 7D
AA EC FF 7D E2 52 8B B7 65 EE 2C 69 07 1D D9 14
C5 5A 6B 5A BC EF 34 12 C4 0D 7D 4E AA DD 19 0A
2B 5F 8B CE 06 2D A0 6C 76 49 E2 62 AC 4B 04 46
FA E6 58 3E D0 7B 58 F0 8A 9E 67 1B 96 3C B3 93
94 66 8A 44 50 D5 4F F8 49 33 4E BA CA E1 95 24
92 43 85 FC A8 B1 66 6F 46 57 BD A5 B3 1E 1B 47
5B 95 EB E7 8C 41 25 DC 88 9D 66 72 36 6B C1 D8
E8 60 59 BA 1F BD 66 A7 3C A3 1D 08 DE CF EB 02
10 90 FD 9A F9 51 83 6C 22 79 6F 79 D7 98 52 43
DD 1E 66 AB E1 F0 E2 E4 85 0D 5F E5 B9 83 07 E0
84 9C B8 3A 60 1E 00 31 8B E9 7B 9B 6E 56 F0 84
81 A7 AE AE BE B2 56 0A C3 B8 DE B8 5C 8A 09 83
4C 9F 12 D3 DE C2 08 F2 79 CF 71 51 B3 E5 F0 D2
47 12 0E DF 98 B2 5C 02 E7 E3 4D B3 6B 20 91 0D
7C 0E E2 95 2E 7A 29 E2 7C C0 A8 9A B6 25 C1 FB
E5 EB A5 A0 F6 E2 E6 A0 70 4E E5 8F DE 1E 9C 33
29 2F DA 85 E0 9A C2 F6 6F 71 A9 84 E7 F9 61 29
50 3A 0A 65 C3 BD 91 CC 7E 52 69 84 12 27 6C 97
0C 9C FC 60 32 58 7D BD 2E 4F 5A 36 97 ED 34 5A
35 2F A8 ED DC A0 67 F0 FE 17 C9 E0 6E D6 D1 9D
58 C2 E0 81 6F C1 7F E9 38 5C EC 5A 30 08 00 CB
C3 65 2F A9 78 6D F5 C0 D1 34 8E 99 C8 52 85 E4
F7 06 FD E7 1B 14 9F 97 BD D9 97 29 18 8A 2A E4
76 AA 36 2D CE 4E E4 D0 84 69 65 22 0C 9B A4 42
```

図 3　暗号文 2 を 16 進表示したもの（cryptan2.txt）

あなた「了解しました。こちらの cryptan2.txt もテキストファイルでいただけますね」

依頼者「もちろんです。暗号文 2 を作り出した暗号プログラムの構成図 2 がこちらです（図 4）」

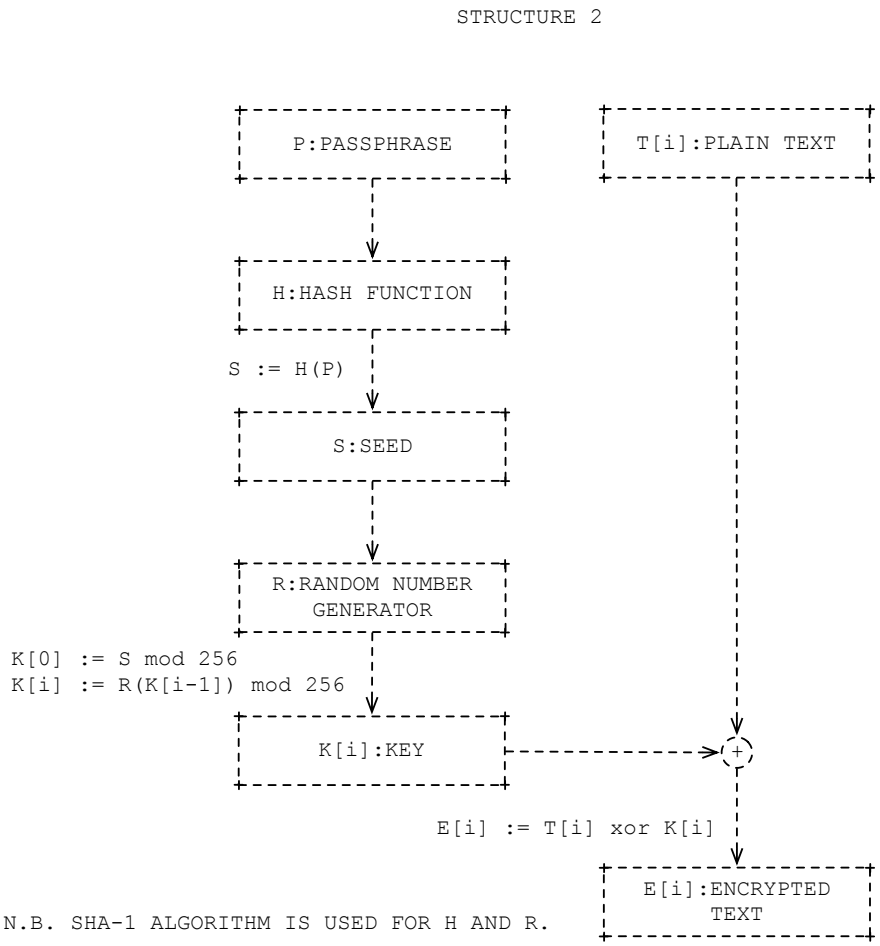


図 4　暗号プログラムの構成図 2

あなた「おっと、この PASSPHRASE というのは……長さが任意のパスフレーズでしょうか」

依頼者「それを推測するのはあなたの仕事かと思いますが（キッ）」

あなた「は、はあ……では、整理させてください。私の仕事はこういうことですね」

- 暗号前の文章は二つとも ASCII コードで書かれていた。
- 「暗号プログラムの構成図」は与えられているが、詳細部分は推測する。
- その上で、二つの暗号文を暗号解読し、暗号前の文章を復元する。

依頼者「その通りです。よろしくお願いいたします」

ミッションはこのようにして始まりました……。