A Method for QR Code Decryption Based on SMS4

Ye Yuan

Department of Computer Science, North China Electric Power University, Baoding 071000, China

hong198520@163.com

Keywords: SMS4; QR code.

Abstract. The QR code to pay not only represents people’s new way of life, is also one of hot topics in the study of the current electronic payment field. But for the sake of lack of mature and safe payment scheme, being unable to further open up capital chain to complete settlement of funds to guarantee the safety of the payment process, Domestic QR code payment has not been popular, still mainly stays in the information application level such as retrieving goods, serving as a proof of payment. This paper uses the SMS4 algorithm to encrypt plaintext of QR codes, has effectively solved security issues about short key length in DES.

1. Introduction

With the development of economy and the maturity of the IT technology, the business model paid in QR code for the media gradually enters into people's horizons. The QR code to pay not only represents people’s new way of life, is also one of hot topics in the study of the current electronic payment field. You just need to scan the qr code, which allows the customer in a short period of time to finish all the process from order to pay just through phone. Its convenience has won a wide recognition of industry. But for the sake of lack of mature and safe payment scheme, being unable to further open up capital chain to complete settlement of funds to guarantee the safety of the payment process, Domestic QR code payment has not been popular, still mainly stays in the information application level such as retrieving goods, serving as a proof of payment. Additionally, taking the recent news into consideration, for example, the Central Bank exerted a halt on QR code and using the QR code payment led to being cheated, people are worried about the safety of the qr code payment.

QR codes originated in Japan Denso Company, is a kind of matrix QR code, with large information capacity, high reliability, low cost advantages. QR codes in addition to the English character, also can represent Chinese characters, images and other information medium, widely used in transportation, communications, financial, medical, and service industries. With the widely application of the qr code, its security problem is increasingly serious. The most notable is the customer service center of China railway’s train ticket real-name system carried out in recent years. In the beginning, the personal information on the QR code of train ticket entirely use clear storage. Ordinary users can access the personal information only by common sweep code software, which seriously damages citizens’ personal privacy. So as QR codes are widely used, its security problem more cannot be ignored.

2. The existing research

However, researches of encryption method directing at QR code are not much, and among them Zhang Dinghui in 2011 came up with a theory using DES encryption algorithm to encrypt binary image of QR codes. The method using the classical cryptography algorithm DES as the encryption algorithm, is widely used nowadays. But the encryption speed is slow, and the security of 56 secret key length in the rapid development of computer technology is slightly insufficient. The table 1 shows that even with a brute force cracking, cracking time of DES is only 1 hour.

Table 1 Exhaustive search key time

Key lengths(bit)	Encryption algorithm	Alternative Number of key	Time taken (encrypt 109 times per second)	Time taken (encrypt 1013 times per second)
56	DES	2^{56}=7.2*10^{16}	2^{55}ns=1.125years	1 hour
128	AES/SMS4	2^{128}=3.4*10^{38}	2^{127}ns=5.3*10^{21}years	5.3*10^{17}years
168	3DES	2^{168}=3.7*10^{50}	2^{167}ns=5.8*10^{33}years	5.8*10^{29}years
192	AES	2^{192}=6.3*10^{57}	2^{191}ns=9.8*10^{40}years	9.8*10^{36}years
256	AES	2^{256}=1.2*10^{77}	2^{255}ns=1.8*10^{60}years	1.8*10^{56}years

3. The introduction of the dense SMS4 algorithm

This paper uses the SMS4 algorithm to encrypt plaintext of QR codes.SMS4 algorithm is the same as the DES. It is also a kind of grouping symmetrical encryption algorithm, in 128, for a set, and the secret key length is 128 bits. If you use a brute force cracking, it will take you 5.3*10^{17} years to crack it, which guarantees the safety. Both the encryption algorithm and key expansion algorithm adopt 32 rounds of nonlinear iterative structure. The structure of decryption algorithm and the structure of the encryption algorithm are identical except for the reverse sequence of the use of round key, and the order of decryption keys is the reverse order of encryption keys.

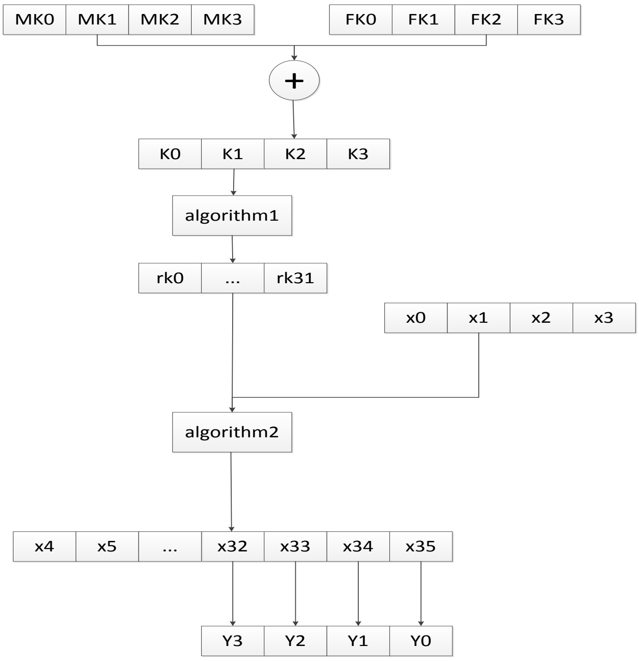


Figure 1 algorithm flow chart

4. Arithmetic step

Step 1, let secret key $MK_i \ (i=0,1,2,3)$ xor the steady index $FK_i \ (i=0,1,2,3)$, we can get the K_0 to K_3.

Step 2, use K_0 to K_3 to get 32 round secret key rk_0 to rk_{31} by arithmetic 1.

Step3, through arithmetic 2 we use the round key and plaintext X_0 to X_3 to get X_4 to X_{35}.

Step4, selcet the final four index as the cryptograph Y_3, Y_2, Y_1, Y_0.

Arithmetic 1 is called round-key-expend arithmetic and we can get round key rk_0 to rk_{31} by using it. Arithmetic is expressed as follow:

$$rk_i = K_{i+4} = K_i \oplus T^{'}(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i)$$

Arithmetic 2 is the round-function-arithmetic, it’s expressed as follow:

$$F(X_0, X_1, X_2, X_3, rk) = X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus rk)$$

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i) \qquad (i = 0,1,...31)$$

Through arithmetic2, we will get x4-x35. Finally, let the cryptograph (Y_3 , Y_2 , Y_1 , Y_0)= $(X_{35}, X_{34}, X_{33}, X_{32})$.

$T(.)$ and $T^{'}(.)$ are replacement synthesis function, can be indicated as follow:

$T(.) = L(\tau(.))$

$\tau(.)$ is nolinear transformation while $L(.)$ is linear transformation. $\tau(.)$ will applied reference the Sbox[1]. The Sbox is announced by the national bureau of password.

$L(.)$ indicated as follow :

$$C = L(B) = B \oplus (B <<< 2) \oplus (B <<< 10) \oplus (B <<< 18) \oplus (B <<< 24)$$

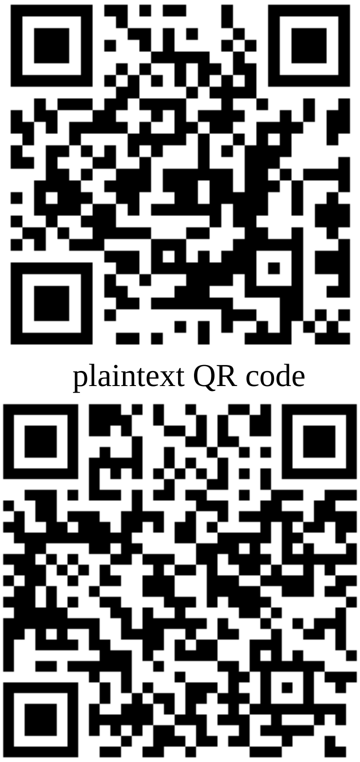
And $L^{'}(.)$ indicated as follow:

$$C = L^{'}(B) = B \oplus (B <<< 13) \oplus (B <<< 23)$$

5. Applied SMS4 to encryption QR codes

Step 1, converting the string “hellothenewworld” into plaintext QR code by using a normal QRpager gold. We regard it as a control group. as shown in the figure 2(a).

Step 2, converting the string “hellothenewworld” into cryptographic string, secret key is “hellothenewworld” too. Then using a normal QRpager gold to transform the cryptograph into QR code, as shown in the figure 2(b).



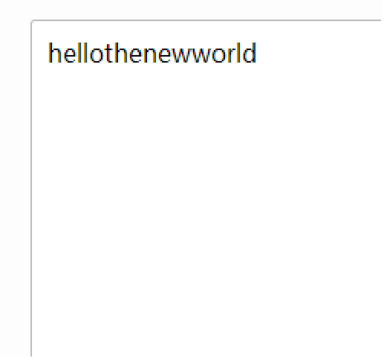
plaintext QR code

(b) encryption QR code

Figure 2 QR code

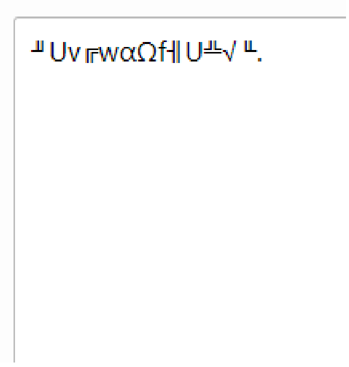
6. Decryption

We will decode the two QR code obtain form above-mentioned. We get two pices of information as follow by using a mobile phone built-in decoder. It is quite clear that we can get the right information from plaintext QR code while we just get a messy code when we decode the cryptographic string.



hellothenewworld

(a) plaintext QR code



╜Uv╓wαΩf╢U╩√╙.

(b) encryption QR code

Figure 3 QR code

References

[1] SMS4 cipher algorithm using in Wireless local area network (LAN) products, National commercial password management office, http: //www.oscca.gov.cn/.

[2] William Stallings, network security essentials: applications and standards, 5e, PEARSON EDUCATION ASIA LIMITED and TSINGHUA UNIVERSITY PRESS, Beijing, 2013.

[3] Song Yang, Research of QR Code Encryption Method Based on Cellular Automata, MS. Harbin University of Science and Technology, March, 2014.