Word Count: 1082

Plagiarism Percentage 18%

Matches

1 **World Wide Web Match**
View Link

2 **World Wide Web Match**
View Link

3 **World Wide Web Match**
View Link

4 **World Wide Web Match**
View Link

5 **World Wide Web Match**
View Link

6 **World Wide Web Match**
View Link

7 **World Wide Web Match**
View Link

Suspected Content

A Brief Survey on RC4 Cryptography Prashanth A R Dept. of CSE PES University Bangalore, India prashanthathunt@gmail.com Abstract—RC4 may be a stream cipher which was most generally accepted for its structural simplicity. it's high rate of encryption and decryption rate i.e speed and efficiency. There were several reports on RC4 algorithm vulnerabilities and further proposals on modified RC4 algorithm. In spite of of these vulnerabilities still RC4 is been utilized in TSL web connections. There were many efforts on removing weakness of RC4 like biased key , key collisions, key recovery etc , specifically from WEP ,so WPA standard was introduced to over come these vulnerabilities . WPA was again proved insecure due to TB data injection attack.researchers are performing on RC4 from past 20 years but still the attraction towards RC4 has been alive. Index Terms—RC4 , cryptography , stream cipher , algorithm , survey I. INTRODUCTION RC4(Rivest Cipher 4) is additionally referred to

as ARC4 or ARCFOUR meaning Alleged RC4. RC4 may be a stream cipher , which is understood for its simplicity and performance in software

2

. RC4 became a neighborhood of

encryption protocols and standards, like WEP in 1997 , in 2003 WPA

2

was released

for wireless cards , and in 1995 SSL and its successor TLS in 1999 ,TLS and SSL was

2

a great success until it was prohibited in 2015 due to RC4 attack or cracking RC4 which was main cryptography used in SSL/TLS. RC4 was very easy to implementation on software and hardware devices. RC4 may be a symmetric encryption where single key's shared between both the parties to encrypt and decrypt the cipher [1] Secret key ciphers can be classified into 2 main branches a.stream ciphers b. block ciphers.RC4 may be a Stream cipher which suggests it encryption takes palace

bit by bit where as in block ciphers it the encryption

7

will happen during a fixed size block. The strength of the stream cipher depends on the random key stream generated which is then xor-ed with the plain text. II. ALGORITHM RC4 algorithm has 2 main components

KSA(Key- scheduling algorithm) and PRGA(Pseudo-random generation algorithm) . the

6

key key's passed though KSA and PRGA the output is bitwise xored with plaintext. it's almost like just one occasion pad expect that the pseudorandom number generated by PRGA is employed instead of prepared streams. KSA is employed for initializing the S array , the output is given to PRGA. KSA algorithm

For as many iterations as are needed, the PRGA modifies the state and outputs a byte of the keystream. In each iteration, the PRGA. PRGA algorithm the

2

output K stream is xored with the plaintext to encrypt the info , or it's xored with ciphertext to decrypt the info Fig. 1. RC4 flow diagram III. MODIFICATION APPROACHES

PSEUDO CODE I KSA OF IMPROVED RC4 PROPOSED BY JIAN XIE ET AL:[

4

2].

PSEUDO CODE II PRGA OF IMPROVED RC4 PROPOSED BY JIAN XIE ET AL:[4

2]. Many more modification on RC4 are made in decades to improve security as well as speed . IV. SECURITY ANALYSIS •

RC4 is mainly used in WLAN security protocols 5

be- cause of it performance and low computation power need. Wired equivalent privacy (WEP) is the primary Fig. 2. RC4

security protocol used for Wi -Fi security in IEEE 802.11 LANs and is based on RC4 encryption algorithm. due to the amount of attacks on WEP such as; related key attacks[3], Fluhrer, Mantin and Shamir attack (FMS)[4], Korek practical attacks[5], Mantin attack on RC4 [6] and WEP,and 1

many more therefore

WEP was announced as an insecure protocol. 5

WPA was more secure by

defended against many attacks in WEP. • WPA has again announced to be a weak protocol due to TB data injection attacks[7], and SVV attacks[8]]. new protocol WPA2 was 1

announced which uses AES (type of symmetric cipher called Advance encryption standard which is a type of

block cipher) as an encryption algorithm instead of RC4. Even Though WPA2 may be a secure protocol, removing many vulnerabilities of WEP. 1

hardware based applications which uses WEP and WPA with RC4 were cost effective. •

Further a replacement protocol WPA2 was proposed by the WiFi alliance which uses AES block cipher as an standard encryption algorithm instead of RC4. Though WPA2 could also be a secure protocol, removing many vulnerabilities of WEP 1

and WPA but its hardware based applications are not cost effective as compare to WEP and WPA where RC4 cryptography algorithm is used as a

basis. • RC4 is additionally widely used and

accepted in web security. it' s utilized in Transport layer security (TLS) /SSL to supply security over the web . The RC4 is understood to the simplest choice for TLS/SSL because it can mitigate many attacks on the protocol. However recently in 2013 and 2014, a replacement security attack[9] on RC4 of

1

Although there has been many successful security breaches within the protocols using RC4, but the striking combination of style elegance and robustness of RC4 has made it most widely accepted protocol for last

1

20 years . V. APPLICATION RC4 was widely utilized in WLAN connection in WEP and WPA . WPA2 uses AES for better security . RC4 was been utilized in TLS/SSL before 2015 which is not any more utilized in web security. versions of RC4 is employed in bluetooth , radios and lots of more small devices which has low computation power but yet security is vital There are many variant of RC4 like RC4A proposed by Bart Preneel and Souradyuti Paul [10] Variably Modified Permutation Composition (VMPC) [11] Spritz by Rivest, Ron; Schuldt, Jacob (27 October 2014)[12]. RC4+ by Goutam Paul and Subhamoy Maitra (19 September 2008)[13] CONCLUSION In this article I even have presented a fast study of RC4 ,about is robust feature and its weaknesses . How easy it is to implement on hardware and software .I had presented a wide kinds of RC4 algorithms improving the security aspects of RC4 . it had been widely utilized in wireless communication(like WEP and WPA) and web security like TLS/SSL until it had been declared to be insecure . In

spite of all the improvements / developments reported within the literature, there are still many open research issues and challenges related to searches of more key collisions in key stream, biases, and key recovery attack on WPA .The conclusion is there'

3

s still research happening , on RC4 to Fig. 3. list of known weakness of RC4 make it more efficient and robust encryption algorithm. ACKNOWLEDGMENT Thanking the PES Institution and therefore the Teachers for his or her support, Guidance and encouragement.