CS6530: Cryptography Basic: Assignment - 1

SNIGDHA BOSE
CS21M502

A8.2)

generator: $X_{n+1} = (aX_n) \bmod 2^4$

$m = 2^4 = 16$
$c = 0$
$0 < a < 16$
taking $X_0 = 1$

a) Maximum period $= 2^{4-2} = 4$

b) for $a = 5$

$1 \{ 5, 9, 13, 1, 5, 9, 13, 1 \ldots \}$

period = 4

for $a = 11$

$1 \{ 11, 9, 3, 1, 11, 9, 3, 1 \ldots \}$

period = 4

for maximum value of a, $a = 5$ or $a = 11$

c) The seed must be odd.

A8.4) let Initial seed, $X_0 = 1$,

for $X_{n+1} = (6 X_n) \bmod 13$

sequence: $1 \{ 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1 \ldots \}$

period = 12

for $X_{n+1} = (7 X_n) \bmod 13$

sequence: $1 \{ 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1, \ldots \}$

period = 12.

The first sequence appears to be more random. Because of the pattern seen in the second half of the sequence generated by the second generator it appears to be less random, although period of both sequences generated is of size 12.

A.8.6) If we use a key of length 255 Bytes.
First two bytes are zero.

ie $k[0] = 0$
$k[1] = 0$

∴ we have
$k[2] = 255$
$k[3] = 254$
$k[4] = 253$
$k[5] = 252$
⋮
$k[255] = 2$

A.8.7) a) To store i, j & S it requires
$[8 + 8 + (256 \times 8)]$ bits
$= [16 + 2048]$ bits
$= 2064$ bits.

b) The number of states are -
$[256! \times 256^2] \approx 2^{1700}$

This is equal to approx 2^{1700}

∴ 1700 bits required to represent the state.

A.8.8)
a) If we take the first 80 bit of v||c we will get v (initialization vector).

Now, since v, c & k are known, the message can easily be decrypted by using the -
$RC4(v||k) \oplus c$

b) for distinct i≠j,

If adversary notices that $v_j = v_i$,

They will know that same key stream used to encrypt m_i & m_j

So, the messages (m_i, m_j) may be vulnerable and can be decrypted.

c) As the key is fixed, the key stream will vary with the IV which will be selected at random.

$\therefore 2^{40}$ messages. (By Birthday Paradox)

d) 2^{40} messages can be encrypted using the key k, after which key should be changed.

PDF Created Using

Camera Scanner

Easily Scan documents & Generate PDF

https://play.google.com/store/apps/details?id=photo.pdf.maker