Computer Security

Stream Cipher

Hyoungshick Kim

Department of Software

College of Software

Sungkyunkwan University

Symmetric key crypto

- Stream cipher — based on one-time pad
  - Except that key is relatively short
  - Key is stretched into a long keystream
  - Keystream is used just like a one-time pad
  - RC4, A5/1, and etc.
- Block cipher — based on codebook concept
  - Block cipher key determines a codebook
  - Each key yields a different codebook
  - Employs both “confusion” and “diffusion”

Stream Ciphers: making OTP practical

Idea: Replace “random” key by “pseudorandom” key

$PRG\ is\ a\ fuction\ G: \{0, 1\}^s \rightarrow \{0, 1\}^n$

Generate a pseudo random key using a random seed!

Encryption: $c = G(k) \oplus m$

Security will depend on specific PRG G

Quiz

Can a stream cipher have perfect secrecy?

No, since the key is shorter than the message

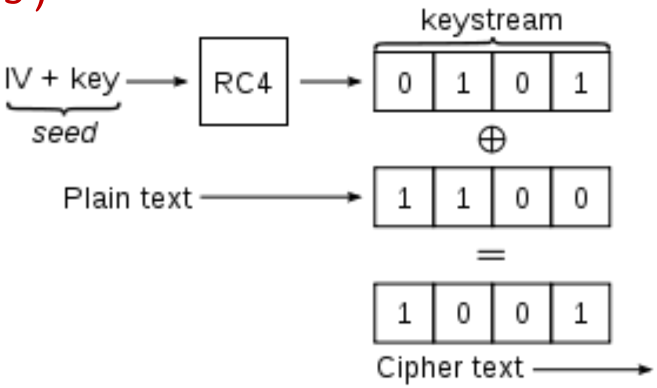
RC4 stream cipher

- A proprietary cipher owned by RSA, designed by Ron Rivest in 1987
- Became public in 1994
- Simple and effective design
- Variable key size (typical 40 to 256 bits)
- Output unbounded number of bytes
- Widely used (SSL/TLS, wireless WEP)
- Extensively studied, not a completely secure PRNG
- Newer Versions: RC5 and RC6

Stream cipher example - RC4

- Key stream generation:
  - (S[] is permutation of 0,1,...,255)

```
i:= i+1    (mod 256)
j:= j+s[i](mod 256)
swap(s[i],s[j])
t:= s[i]+s[j]  (mod 256)
k:= s[t]
```



- Idea: systematically keep swapping and producing output bytes (i.e., S [ ])

Security of RC4

- RC4 is not a truly pseudorandom generator.
- The keystream generated by RC4 is biased.
  - The second byte is biased toward zero with high probability.
  - The first few bytes are strongly non-random and leak information about the input key.
- Defense: Discard the initial *n* bytes of the keystream.
  - Called “RC4-drop[*n*-bytes]”.
  - Recommended values for *n* = 256, 768, or 3072 bytes.

Trends of stream ciphers

- Stream ciphers were popular in the past
  - Efficient in hardware
  - Speed was needed to keep up with voice, etc.
  - Today, processors are fast, so software-based crypto is usually more than fast enough
- Future of stream ciphers?
  - Shamir declared “the death of stream ciphers”
  - May be greatly exaggerated…

Questions?

Sungkyunkwan
Campus
established
University
university
Sciences
campus
School
Suwon
Seoul
Natural
Graduate
English
constructed
Korean
Social
Global
Building
Institute
edit
Professors
Confucian
Humanities
lecturers
Business
Korea
Zone
schools
Science
Administration
Academic
ASLE-Korea
also
two
four
Hall
Course
Joseon
located
Engineering
Education
Anniversary
establishment
University's
Advanced
Language
heart
Samsung
Technology
symbol
city
trees
now
one