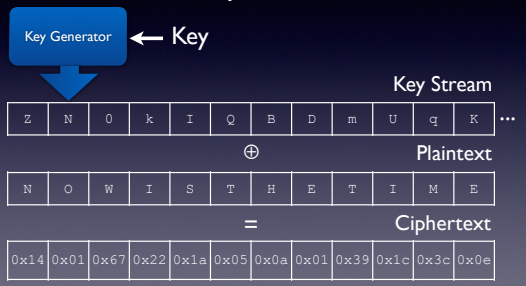
Stream Ciphers

CMSC 426/626 - Computer Security

Outline

- Properties of stream ciphers
- Examples

Generic Stream Cipher



Properties

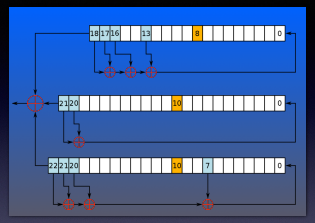
- The *period* of a key generator is how many key bytes (or bits) it can produce before the stream repeats. The period needs to be large.
- The key stream should be statistically indistinguishable from a random sequence.
- The secret (input) key must be long enough to prevent a brute force attack.

Some Stream Ciphers

- We've seen two already:
  - Block Cipher in CFB or CTR mode
- A5/1
- RC4

A5/1

- Used to encrypt the air interface in GSM.
- The A5/1 cipher generates a stream of pseudo-random bits.
- Built from three shift registers - 19, 22, and 23 bits long.
- Registers step irregularly according to the *motion bits*.



- Registers “step or stutter” according to a majority vote of the motion bits (orange).

RC4

- Created by Ron Rivest, it is the most commonly used stream cipher.
- Produces a stream of pseudo-random bytes.
- Is fast and easy to implement.

RC4 Run-Up

- The run-up creates a pseudo-random permutation that is used in key generation.
- Input `key`, an array of bytes; output array `s`.

```
s = []
for i in range(256):
    s.append(i)

j = 0
for i in range(256):
    j = (j + s[i] + key[i % len(key)]) % 256
    # swap s[i] and s[j]
    s[i], s[j] = s[j], s[i]
```

RC4 Key Generation

- Uses `s[]` from the run-up to generate key.

```
i = 0
j = 0
outdata = []
for c in data:
    i = (i + 1) % 256
    j = (j + s[i]) % 256
    # swap s[i] and s[j]
    s[i], s[j] = s[j], s[i]
    k = s[(s[i] + s[j]) % 256]
    outdata.append(c ^ k)
```

RC4 Speed

- RC4 is roughly twice as fast as AES.
- Use `openssl speed` command:

```
The 'numbers' are in 1000s of bytes per second processed.

 type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes
 rc4              325154.19k   343987.63k   355510.47k   362255.13k   363893.62k
 aes-128 cbc      136176.67k   142857.31k   143824.91k   142676.45k   143104.28k
 des cbc           71311.72k    72436.07k    73486.61k    73745.93k    72224.61k
```

Fluher, Mantin, Shamir

- Published in 2001; can recover secret key **under certain conditions**.
- Applies when an *Initialization Vector* (IV) is used to prevent *depth*, e.g. as used in WEP.
- IV is known to attacker; can reveal information about permutation *S*.
- Improved significantly in 2005 by Andreas Klein.

Homework will be posted on the website.