Introduction to Cryptography
CS 355
Lecture 9

One Time Pad
One-Time Pad

- Basic Idea: Extend Vigenère cipher so that the key is as long as the plaintext
  - No repeat, cannot be broken by finding key length + frequency analysis
- Key is a random string that is at least as long as the plaintext
- Encryption is similar to Vigenère
One-Time Pad

Plaintext space =
Ciphertext space =
Keyspace = $(Z_m)^n$
Key is chosen randomly
Plaintext $X = (x_1 \ x_2 \ \ldots \ x_n)$
Key $K = (k_1 \ k_2 \ \ldots \ k_n)$
$Y = (y_1 \ y_2 \ \ldots \ y_n)$
$e_k(X) = (x_1+k_1 \ x_2+k_2 \ \ldots \ x_n+k_n) \mod m$
$d_k(Y) = (y_1+k_1 \ y_2+k_2 \ \ldots \ y_n+k_n) \mod m$
How Good is One-Time Pad?

- Intuitively, it is secure …
- The key is random, so the ciphertext is completely random
Shannon (Information-Theoretic) Security

- Basic Idea: Ciphertext should provide no “information” about Plaintext
  - Precise definition will be given towards the end of the course
- We also say such a scheme has perfect secrecy.
- One-time pad has perfect secrecy
  - E.g., suppose that the ciphertext is “Hello”, can we say any plaintext is more likely than another plaintext?
What about the Ciphers We Have Studied

• Why Shift cipher does not have perfect secrecy?

• Why Vigenère cipher does not have perfect secrecy?
Key Randomness in One-Time Pad

• One-Time Pad uses a very long key, what if the key is not chosen randomly, instead, texts from, e.g., a book is used.
  – this is not One-Time Pad anymore
  – this does not have perfect secrecy
  – this can be broken easily

• The key in One-Time Pad should never be reused.
  – If it is reused, it is Two-Time Pad, and is insecure!
The “Bad News” Theorem for Perfect Secrecy

• Perfect secrecy $\Rightarrow$ key-length $\geq$ msg-length

• Difficult to use in practice
The Binary Version of One-Time Pad

Plaintext space = Ciphertext space =
Keyspace = \{0,1\}^n
Key is chosen randomly
For example:

- Plaintext is 11011011
- Key is 01101001
- Then ciphertext is 10110010
Bit Operators

- Bit AND
  \[ 0 \land 0 = 0 \quad 0 \land 1 = 0 \quad 1 \land 0 = 0 \quad 1 \land 1 = 1 \]

- Bit OR
  \[ 0 \lor 0 = 0 \quad 0 \lor 1 = 1 \quad 1 \lor 0 = 1 \quad 1 \lor 1 = 1 \]

- Addition mod 2 (also known as Bit XOR)
  \[ 0 \oplus 0 = 0 \quad 0 \oplus 1 = 1 \quad 1 \oplus 0 = 1 \quad 1 \oplus 1 = 0 \]

- Can we use operators other than Bit XOR for binary version of One-Time Pad?
Stream Ciphers

- In OTP, a key is described by a random bit string of length $n$
- Stream ciphers:
  - Idea: replace “rand” by “pseudo rand”
  - Use Pseudo Random Number Generator
  - PRNG: $\{0,1\}^s \rightarrow \{0,1\}^n$
    - expand a short (e.g., 128-bit) random seed into a long (e.g., $10^6$ bit) string that “looks random”
  - Secret key is the seed
  - $E_{\text{seed}}[M] = M \oplus \text{PRNG}(\text{seed})$
Properties of Stream Ciphers

• Does not have perfect secrecy
  – security depends on PRNG

• PRNG must be “unpredictable”
  – given consecutive sequence of bits output (but not seed), next bit must be hard to predict

• Typical stream ciphers are very fast

• Used in many places, often incorrectly
  – SSL (RC4), DVD (LFSR), WEP (RC4), etc.
Fundamental Weaknesses of Stream Ciphers

• If the same stream is used twice ever, then easy to break.
• Highly malleable
  – easy to change ciphertext so that plaintext changes in predictable, e.g., flip bits
• Weaknesses exist even if the PRNG is strong
Coming Attractions …

• Linear Feedback Shift Register (LFSR)

• Recommended reading for next lecture:
  – Trappe & Washington: 2.10