Lecture 7.1: Private-key Encryption

Private-key Encryption

- Alice and Bob share a secret $s \in \{0,1\}^n$

Private-key Encryption

- Alice and Bob share a secret $s \in \{0,1\}^n$
- Encryption and Decryption algorithms are efficient

Private-key Encryption

- Alice and Bob share a secret $s \in \{0,1\}^n$
- Encryption and Decryption algorithms are efficient
- Encryption of a message when decrypted provides the original message

Private-key Encryption

- Alice and Bob share a secret $s \in \{0,1\}^n$
- Encryption and Decryption algorithms are efficient
- Encryption of a message when decrypted provides the original message
- "Encryption of any message m_0 is indistinguishable from encryption of any other message m_1" to an eavesdropper

Private-key Encryption

- Alice and Bob share a secret $s \in \{0,1\}^n$
- Encryption and Decryption algorithms are efficient
- Encryption of a message when decrypted provides the original message
- "Encryption of any message m_0 is indistinguishable from encryption of any other message m_1" to an eavesdropper
- Design a predictive experiment to summarize this concept

- Alice and Bob share a secret $s \in \{0,1\}^n$
- Encryption and Decryption algorithms are efficient
- Encryption of a message when decrypted provides the original message
- "Encryption of any message m_0 is indistinguishable from encryption of any other message m_1" to an eavesdropper
- Design a predictive experiment to summarize this concept
- Formally, for all n.u. PPT $\mathcal{A}$:

$$\Pr\left[\begin{array}{c} s \leftarrow \{0,1\}^n, \\ (m_0,m_1) \leftarrow \mathcal{A}, \\ b \xleftarrow{\$} \{0,1\} \end{array} : \mathcal{A}(Enc(m_b)) = b\right] \leqslant \frac{1}{2} + \mathrm{negl}(n)$$

One-time Pads

- Alice and Bob share $s \xleftarrow{\$} \{0,1\}^n$

One-time Pads

- Alice and Bob share $s \xleftarrow{\$} \{0,1\}^n$
- Encoding of $m \in \{0,1\}^n$ using private-key s is: $\mathrm{Enc}(m; s) := m \oplus s$

One-time Pads

- Alice and Bob share $s \xleftarrow{\$} \{0,1\}^n$
- Encoding of $m \in \{0,1\}^n$ using private-key s is: $\mathrm{Enc}(m; s) := m \oplus s$
- We have:

$$\mathrm{Enc}(m_0; s \xleftarrow{\$} \{0,1\}^n) \equiv \mathrm{Enc}(m_1; s \xleftarrow{\$} \{0,1\}^n)$$

One-time Pads

- Alice and Bob share $s \xleftarrow{\$} \{0,1\}^n$
- Encoding of $m \in \{0,1\}^n$ using private-key s is: $\mathsf{Enc}(m; s) := m \oplus s$
- We have:

$$\mathsf{Enc}(m_0; s \xleftarrow{\$} \{0,1\}^n) \equiv \mathsf{Enc}(m_1; s \xleftarrow{\$} \{0,1\}^n)$$

- Why can't we send two messages using the same pad?

One-time Pads

- Alice and Bob share $s \xleftarrow{\$} \{0,1\}^n$
- Encoding of $m \in \{0,1\}^n$ using private-key s is: $\mathrm{Enc}(m; s) := m \oplus s$
- We have:

$$\mathrm{Enc}(m_0; s \xleftarrow{\$} \{0,1\}^n) \equiv \mathrm{Enc}(m_1; s \xleftarrow{\$} \{0,1\}^n)$$

- Why can't we send two messages using the same pad?
- Length of message bounded by n

One-time Pads

- Alice and Bob share $s \xleftarrow{\$} \{0,1\}^n$
- Encoding of $m \in \{0,1\}^n$ using private-key s is: $\mathsf{Enc}(m; s) := m \oplus s$
- We have:

$$\mathsf{Enc}(m_0; s \xleftarrow{\$} \{0,1\}^n) \equiv \mathsf{Enc}(m_1; s \xleftarrow{\$} \{0,1\}^n)$$

- Why can't we send two messages using the same pad?
- Length of message bounded by n
- Story: "Alice and Bob met and shared a secret. Subsequently, they can encrypt messages of total length smaller than the length of the shared secret."

Using PRGs

- Alice and Bob share $s \xleftarrow{\$} \{0,1\}^n$

Using PRGs

- Alice and Bob share $s \xleftarrow{\$} \{0,1\}^n$
- Encoding of $m \in \{0,1\}^n$ using private-key s is: $\mathrm{Enc}(m; s) := m \oplus \mathrm{PRG}(s)$

Using PRGs

- Alice and Bob share $s \xleftarrow{\$} \{0,1\}^n$
- Encoding of $m \in \{0,1\}^n$ using private-key s is:
  $\mathrm{Enc}(m; s) := m \oplus \mathrm{PRG}(s)$
- We have:

$$\mathrm{Enc}(m_0; s \xleftarrow{\$} \{0,1\}^n) \approx \mathrm{Enc}(m_1; s \xleftarrow{\$} \{0,1\}^n)$$

Using PRGs

- Alice and Bob share $s \xleftarrow{\$} \{0,1\}^n$
- Encoding of $m \in \{0,1\}^n$ using private-key s is: $\mathrm{Enc}(m; s) := m \oplus \mathrm{PRG}(s)$
- We have:

$$\mathrm{Enc}(m_0; s \xleftarrow{\$} \{0,1\}^n) \approx \mathrm{Enc}(m_1; s \xleftarrow{\$} \{0,1\}^n)$$

- Can encrypt arbitrarily long messages

Using PRGs

- Alice and Bob share $s \xleftarrow{\$} \{0,1\}^n$
- Encoding of $m \in \{0,1\}^n$ using private-key s is: $\mathsf{Enc}(m;s) := m \oplus \mathsf{PRG}(s)$
- We have:

$$\mathsf{Enc}(m_0; s \xleftarrow{\$} \{0,1\}^n) \approx \mathsf{Enc}(m_1; s \xleftarrow{\$} \{0,1\}^n)$$

- Can encrypt arbitrarily long messages
- Story: "Alice and Bob met and shared a short secret. Subsequently, they can encrypt arbitrarily long messages."

What if Alice and Bob never met?

What if Alice and Bob never met?

Is it even possible to encrypt one bit?

What if Alice and Bob never met?

Is it even possible to encrypt one bit?
Yes! Public-key Encryption (Later in the course)