SHA Functions Serve as One-Way Hash Functions

Instead, we **use** a **function that**

1. **generates bits that seem random**,
2. is effectively **impossible to invert**, and
3. generates enough bits that **guessing** them is also effectively **impossible**.

In cryptography, such functions are called **one-way hash functions**.

The SHA (Secure Hash Algorithm) functions are a widely used example.