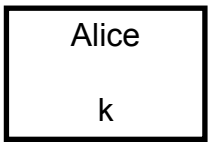
CS 558
Satoe Sakuma
January 26, 2017

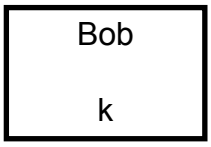
Lecture 3

1. Schemes - how we do encryption and decryption
2. Definition of what it means to be secure
3. Proof of the schema satisfies definition

We will spend most of the class focusing on the first two (schemes and definition)

Encryption Scheme Example: **One Time Pad** (OTP) for 1-bit messages:





To encrypt:
$Enc_k(m) = k \oplus m$
$|m|$ = 1-bit
$|k|$ = 1-bit
m = plain text

To decrypt:
$Dec_k(c) = c \oplus k$

Kerckhoff's Principle

- "The enemy knows your system"
- A crypto system should be secure even if everything about the system is public except for the secret key.

- In the OTP, the key is not known to the adversary. It should be secure even if the system is known.
- "Attack Surface" is small (just the key).
- NIST puts out specifications of encryption for the public because the more people that look at encryption specification and fail, the safer we feel using that encryption.

If we use the one time pad twice

$$\begin{aligned} C_1 &= k \oplus m_1 \\ C_2 &= k \oplus m_2 \\ &\vdots \\ C_l &= k \oplus m_l \end{aligned}$$

Brute Force Attack (try every possible key)

- Only need two tries

$$
\begin{aligned}
c_1 \oplus c_2 &= (m_1 \oplus k) \oplus (m_2 \oplus k) \\
&= m_1 \oplus m_2 \oplus k \oplus kk \oplus k = 0 \\
&= m_1 \oplus m_2 \oplus 0 \\
&= m_1 \oplus m_2
\end{aligned}
$$

Use the OTP to encrypt l-bit message. $m = m_1, m_2 \ldots m_l$

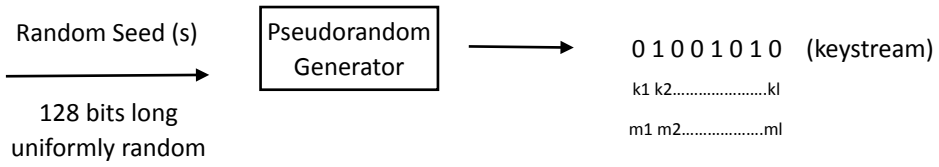
1. Choose l-bit random key
   $k_1, k_2, \ldots k_l$
2. $c = (m_1 \oplus k_1, m_2 \oplus k_2 \ldots m_l \oplus k_l)$

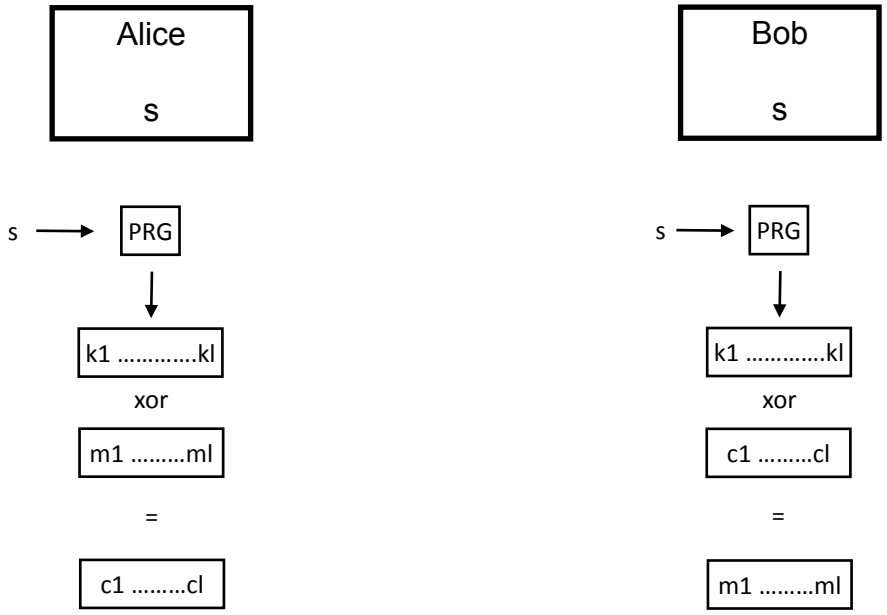
- 2^l tries

Why is this bad?

Example: Let's say the first bit is always zero in an internet packet. Then you know, $m_1 = 0$. Then you can recover the rest of the plain text.

Stream Ciphers



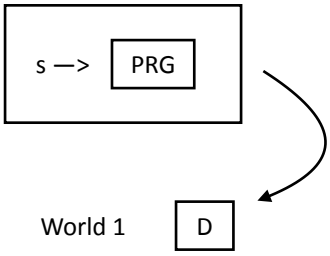


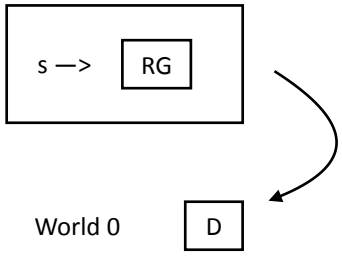
- Randomness comes from s NOT PRG (RC4, Salsa, Cha-Cha)
  Output only looks random if s is random and unknown
- Must throw away key bits after use to avoid same key being used (look at example above)

Secure PRG (theoretical)

- PRG is secure if for all polynomial time adversary cannot distinguish which world he is in.

- Adversary can ask for endless stream of output





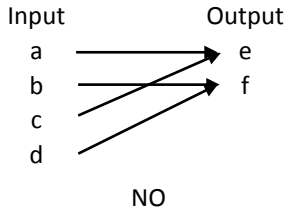
Q: If the definition of secure PRG is theoretical, how can we say it is secure?

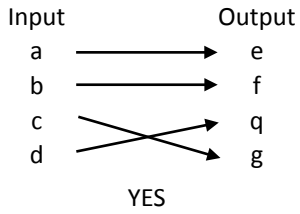
Fields of Crypto:

1. Theoretical/Provable Crypto
2. Cryptanalysis

Abstraction - layers to build higher. The assumptions made are the shakiest part of cypto.

Block Cipher
Pseudorandom Permutation





- Permutations must be a one-to-one function
  - Hash functions are not permutations
- Random Permutation = Take an input and pick a random unique output.
- Permutations of 4 inputs = $4! = 24$, then choose one.