CIS 3362 11/28/22

11/28 - Quantum Cryptography
11/30 - Hash Functions
12/12 - Final Exam Review

Summarize last chat in Code Book
Demonstration - Cryptool

Photons - to know their orientation, you need to use a "reader"

\[ + 1 = 1 \quad - = 0 \]

\[ \times \downarrow = 1 \quad \uparrow = 0 \]

What happens when \( \downarrow \) but read \( + \)?

50% \( \Rightarrow \) read 1, 50% \( \Rightarrow \) read 0.

Sending \[ \rightarrow \]

Alice

It’s near impossible for Eve to observe what’s going on w/o being detected, because her presence affects the qubits.
Goal: for Alice and Bob to exchange a stream of bits for either 1 time pad or a private key scheme knowing that no one else has that stream of bits.

Alice sends Bob \( n \) bits, randomly choosing the reader orientation (doesn't share w/Bob)

\[
\begin{array}{cccc}
1 & 0 & 0 & 1 \\
+ & + & x & + \\
X & X & + & + \\
\hline
W & C & W & W & C
\end{array}
\]

Eve listening \( \rightarrow \)

She'll guess

So on \( \approx n/4 \) bits

Eve will use wrong
Bob will use correct

Afterwards, Alice share Bob's guesses, throw out all wrong guesses. (left \( n/2 \) bits...)

Imagine Alice shares into about the bits w/Bob.

\( n/4 \) bits when Eve guessed wrong, \( 1/2 \) time Bob's answer he's read will disagree w/what Alice sent.

\( n/8 \) bits Bob will get wrong.

\[
\left( \frac{7}{8} \right)^n
\]

where we use \( n \) bits is probability that Eve goes undetected.
We send more than \( n \) bits
Sample \( n \) bits this way randomly.
If no error is detected among all the bits
when Alice + Bob used the same reader, then
we assume Eve wasn't on the line!

\[
\left( \frac{7}{8} \right)^{100} \approx 10^{-6}
\]

If we chose \( n = 400 \Rightarrow \approx 10^{-24} \) (small!)

Example: Send 2000 bits
\[\text{Sample 400 if all ok}\]
Exchange into 1600 readers
\[\text{Keep all bits w/ the correct reader.}\]

In theory would be unbreakable.

Issues: Extremely costly + time consuming
probably issues w/ reliability over distances.