CIS 3362 11/28/22

11/28 - Quantum Cryptography

11/30 - Hash Functions

12/2 - Final Exam Review

→ Summarize last cht in Code Book

Demonstration - Crypt Tool

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

+ | = 1 — = 0

photon

X \ = 1 / = 0

photon

What happens when \ but read + ?

50% ⇒ read 1, 50% → read 0.

sending →

X

↑ put up reader to observe

+

Alice Eve Bob

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 + 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)

|	/	/	\	—	, etc.
1	0	0	1	0	← Eve listening →
+	+	X	X	+	She'll guess

Bob guesses at the reader — wrong reader 1/2 time.

X	X	+	+	+	So on ~ $n/4$ bits Eve use wrong. Bob use correct.
W	C	W	W	C	

Afterwards, ~~A~~ ~~I~~ share ~~Bo~~ Bob's guesses, throw out all wrong guesses. (left $n/2$ bits...)

Imagine Alice shares info about the bits w/Bob. $n/4$ bits where 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 where Alice + Bob used the same reeder, then we assume eve wasn't on the line!

$$\left(\frac{7}{8}\right)^{100} \sim 10^{-6}$$

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

example → send 2000 bits
sample 400 $\overset{\text{if}}{\Longrightarrow}$ all ok
~~[illegible]~~ exchange info 1600 reeders
keep all bits w/ the correct reeder.

In theory would be unbreakable.
Issues: extremely costly + time consuming
probably issues w/ reliability over distances.