Lecture 3 – Perfect Security and One-Time Pad

CS-466 Applied Cryptography
Adam O’Neill
We saw that substitution ciphers cannot hope to achieve even the weakest privacy notion.

But what’s the strongest privacy notion one can hope for? Is there a scheme achieving it?

recovering message from ciphertext is the weakest possible goal!
consider recovering some function of the message
we want to formalize that ciphertext knowledge before seeing ciphertext = knowledge after
Shannon’s Work

Shannon (1948) addressed this in his landmark work, *A Mathematical Theory of Communication*.

This can be viewed as the birth of modern cryptography.
Shannon Security

Say $SE = (1x, E, D)$ with message-space $M$, ciphertext-space $C$, and coin-space $R$ is SHANNON SECURE if we let $c \in C$ be any ciphertext. It must hold that $\Pr_{k \leftarrow R}[E_k(m) = c]$ is the same for all messages $m \in M$.

Game:
- $k \leftarrow R$
- $c' \leftarrow E_k(m)$
- return $(c = c')$

Convence yourself that this implies the adversary’s knowledge before seeing a ciphertext is its knowledge after seeing a ciphertext. $c$ may vary with $c'$. The game outputs 1 is independent of $m$. Probability the game outputs 1 is the same for all messages.
One-Time Pad
Voting Example
Key Re-Use

Suppose the key is used twice. What can the adversary learn?
Another amusing story about the two-time pad is relayed by Klehr [65] who describes in great detail how Russian spies in the US during World War II were sending messages back to Moscow, encrypted with the one-time pad. The system had a critical flaw, as explained by Klehr:

During WWII the Soviet Union could not produce enough one-time pads ... to keep up with the enormous demand .... So, they used a number of one-time pads twice, thinking it would not compromise their system. American counter-intelligence during WWII collected all incoming and outgoing international cables. Beginning in 1946, it began an intensive effort to break into the Soviet messages with the cooperation of the British and by ... the Soviet error of using some one-time pads as two-time pads, was able, over the next 25 years, to break some 2900 messages, containing 5000 pages of the hundreds of thousands of messages that had been sent between 1941 and 1946 (when the Soviets switched to a different system).

The decryption effort was codenamed project Venona. The Venona files are most famous for exposing Julius and Ethel Rosenberg and helped give evidence of their involvement with the Soviet spy ring. Starting in 1995 all 3000 Venona decrypted messages were made public.
One-Time Pad is Malleable
Optimality
Where To?

We have a scheme achieving perfect security and a proof that it’s optimal. (it’s very efficient, and one cannot do better in terms of key-length)

But key-length is completely impractical.

The main key idea of modern cryptography is that it is sufficient to consider efficient adversaries and allow “negligible” success (so small we feel comfortable with it for the foreseeable future)
In other words, security of a practical system must rely not on the impossibility but on the computational difficulty of breaking it.
We might prove, e.g., no attack running in time (or resources) at most \(2^{160}\) succeeds with probability greater than \(2^{20}\).

I.e., attacks could exist as long as it is prohibitive (in time/space, $$$) to mount them.
We measure the running-time of algorithms in the bit-length of their inputs. Not absolute value!

Efficient algorithms have code size, time and space use, etc. which is, e.g., polynomial in the input length (in a formal sense) and “feasible” (in an informal sense).
Factoring Example

Recall

Lower-level primitives

construction

Higher-level primitives

reduction
Quantitative Reductions
Where To?

Our first lower-level primitive, blockciphers.
Next time...