Fundamentals of cryptography

The internet is an open, public system with a lot of data flowing through it.
Even though we all send and store information online, there's some information that we choose to keep private.
In security, this type of data is known as personally identifiable information.
Personally identifiable information, or PII, is any information that can be used to infer an individual's identity.
This can include things like someone's name, medical and financial information, photos, emails, or fingerprints.

Maintaining the privacy of PII online is difficult.
It takes the right security controls to do so.
One of the main security controls used to protect information online is cryptography.
Cryptography is the process of transforming information into a form that unintended readers can't understand.
Data of any kind is kept secret using a two-step process:
encryption to hide the information, and decryption to unhide it.

Imagine sending an email to a friend.
The process starts by taking data in its original and readable form, known as plaintext.
Encryption takes that information and scrambles it into an unreadable form, known as ciphertext.
We then use decryption to unscramble the ciphertext back into plaintext form, making it readable again.

Hiding and unhiding private information is a practice that's been around for a long time.
Way before computers!
One of the earliest cryptographic methods is known as Caesar's cipher.
This method is named after a Roman general, Julius Caesar, who ruled the Roman empire near the end of the first century BC.
He used it to keep messages between him and his military generals private.

Caesar's cipher is a pretty simple algorithm that works by shifting letters in the Roman alphabet forward by a fixed number of spaces.
An algorithm is a set of rules that solve a problem.
Specifically in cryptography, a cipher is an algorithm that encrypts information.

For example, a message encoded with Caesar's cipher using a shift of 3 would encode an A as a D, a B as an E, a C as an F, and so on.
In this example, you could send a friend a message that said, "hello" using a shift of 3, and it would read "khoor."
Now, you might be wondering how would you know the shift a message encrypted with Caesar's cipher is using. The answer to that is, you need the key!

A cryptographic key is a mechanism that decrypts ciphertext.
In our example, the key would tell you that my message is encrypted by 3 shifts.
With that information, you can unlock the hidden message!

Every form of encryption relies on both a cipher and key to secure the exchange of information.
Caesar's cipher is not widely used today because of a couple of major flaws.
One concerns the cipher itself. The other relates to the key.
This particular cipher relies entirely on the characters of the Roman alphabet to hide information.
For example, consider a message written using the English alphabet, which is only 26 characters.
Even without the key, it's pretty simple to crack a message secured with Caesar's cipher by shifting letters 26 different ways.

In information security, this tactic is known as brute force attack, a trial-and-error process of discovering private information.

The other major flaw of Caesar's cipher is that it relies on a single key.
If that key was lost or stolen, there's nothing stopping someone from accessing private information.
Properly keeping track of cryptographic keys is an important part of security.
To start, it's important to ensure that these keys are not stored in public places, and to share them separately from the information they will decrypt.

Caesar's cipher is just one of many algorithms used to protect people's privacy.
Due to its limitations, we rely on more complex algorithms to secure information online.
Our next focus is exploring how modern algorithms work to keep information private.

Revision #1
Created 24 July 2023 07:30:10 by naruzkurai
Updated 15 August 2023 18:44:11 by naruzkurai