CS-501

Introduction to Malware, Threat Hunting & Offensive Capabilities Development

Lecture 12: Cryptography Continued, Ransomware

Agenda for today:

- Another homework Extension, + some hints
- RC4 internals
- Asymmetric Cryptography concepts (RSA, Diffie-Hellman, Elliptic Curves)
- Implant Sessions, registration and python cryptography libraries
- Ransomware
- Mistakes made by ransomware

RC4: Rivest Cipher 4

- Stream cipher commonly used by malware authors due to its ease of implementation
  - Cryptography poses an engineering challenge, as any code you write client side needs to have a counterpart server side. Implementing RC4 is trivial in any language!
- Two components:
  - Key-Scheduling Algorithm (KSA)
  - Pseudo Random Generation Algorithm
- PRNG that generates random bytes from an initial seed (the key)
- Algorithm is synchronous, meaning Client and server need to maintain state information.

KSA

- Initialize an array S of 256 bytes where each byte is set to its index in the array
- We then use the key to create a random permutation of 256 bytes
- That is, we can view S as defining a function, where the input is the index in the array, and the output is the value stored in the array
- That is, initially, S[i] = i for all i=0,...,255, S[input] = output is the identity function
- Using the Key, we randomly swap values inside of the S array
- S is usually called an “S-box”

Generating Psuedo random bytes

Pull data from the Sbox according to the algorithm and update.

Looking at RC4 in Assembly

- Let’s spend some time implementing it!
- We can compile the end result with the -g flag to generate a PDB
- Load it into Ghidra and see if we can identify the relevant portions

Demo

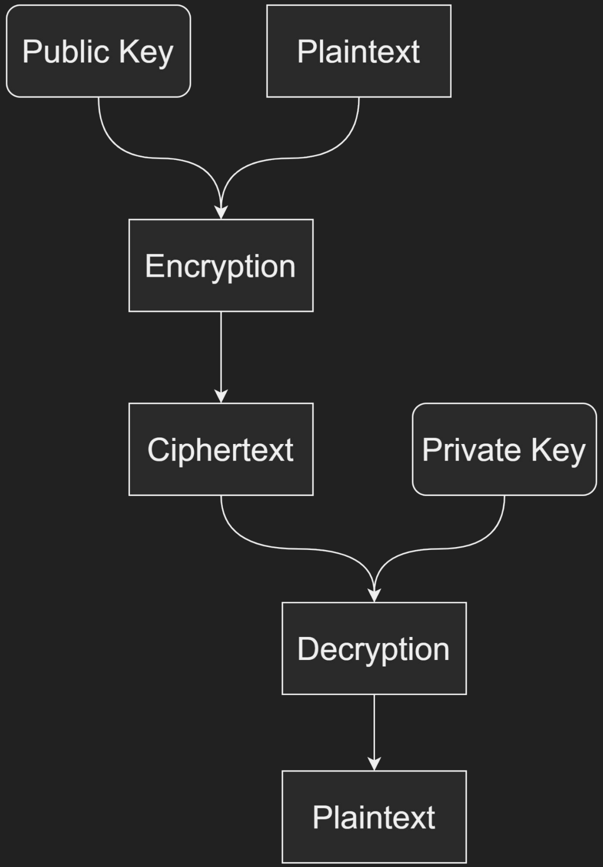
Asymmetric Cryptography (Public Key Cryptography)

How do we securely communicate with someone we have never met before?

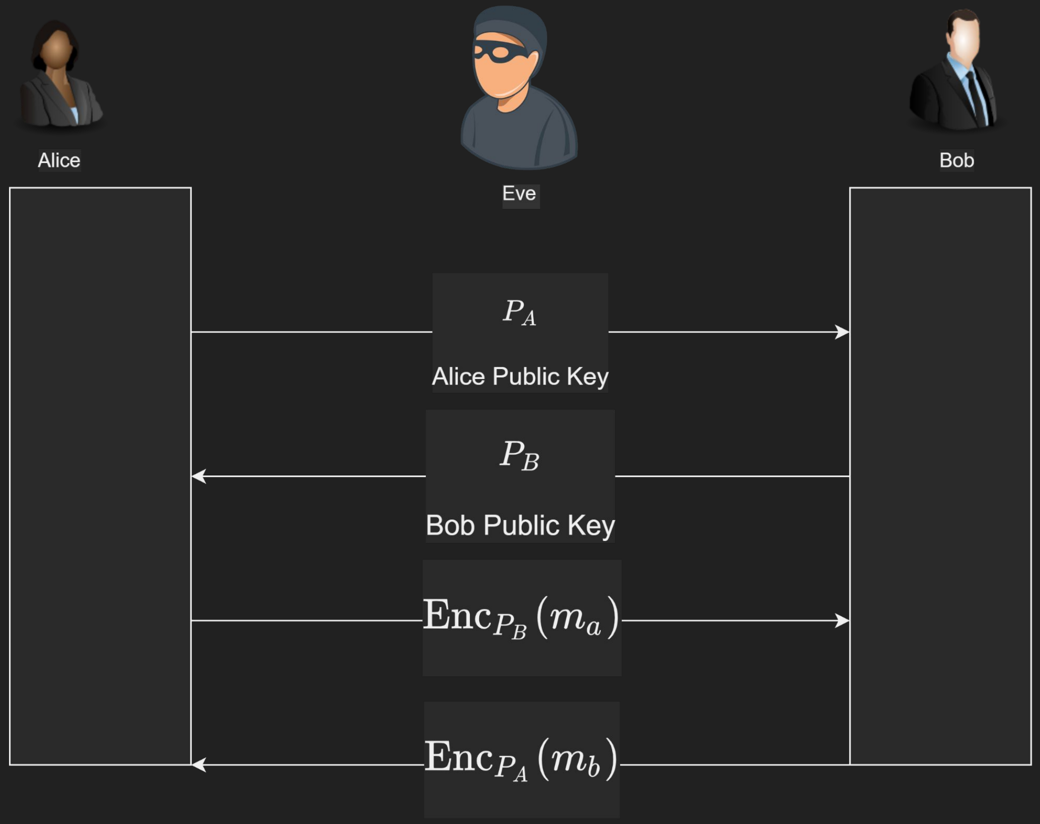
Classic example: how does your browser establish a secure connection with google.com?

Basic Setup

- Now each participant has a public key and a private key
- The public key is published/distributed to the recipient (this is in general pretty hard!)
- Anyone with the public key can encrypt messages
- Only the owner of the private key can decrypt them



Communication with Public Keys



Examples

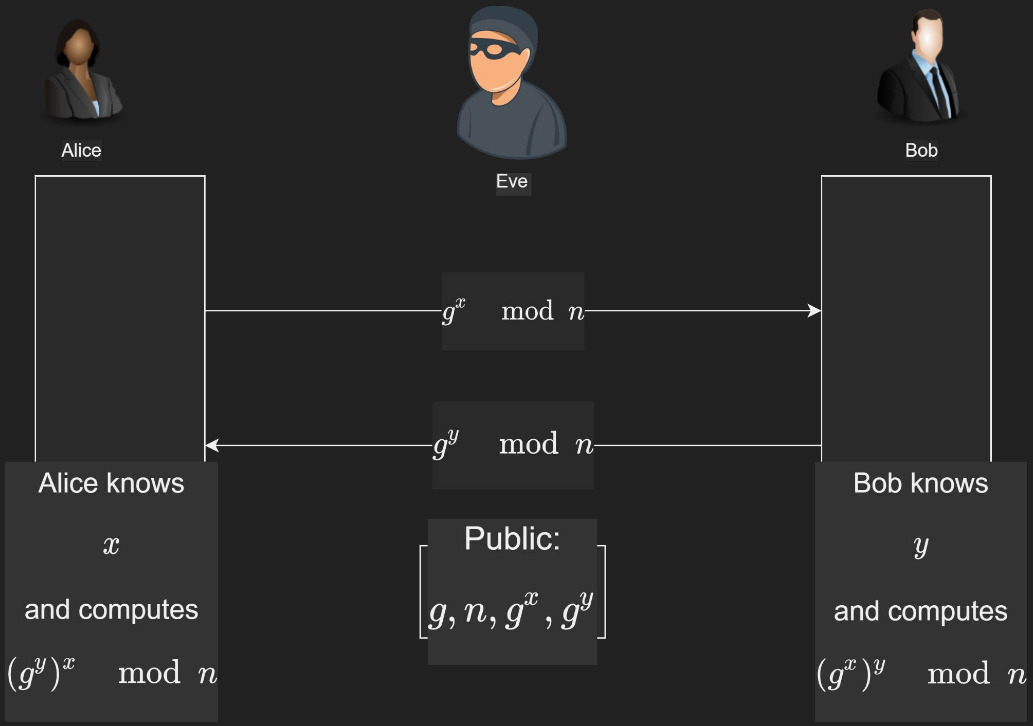
RSA

Diffie Hellman

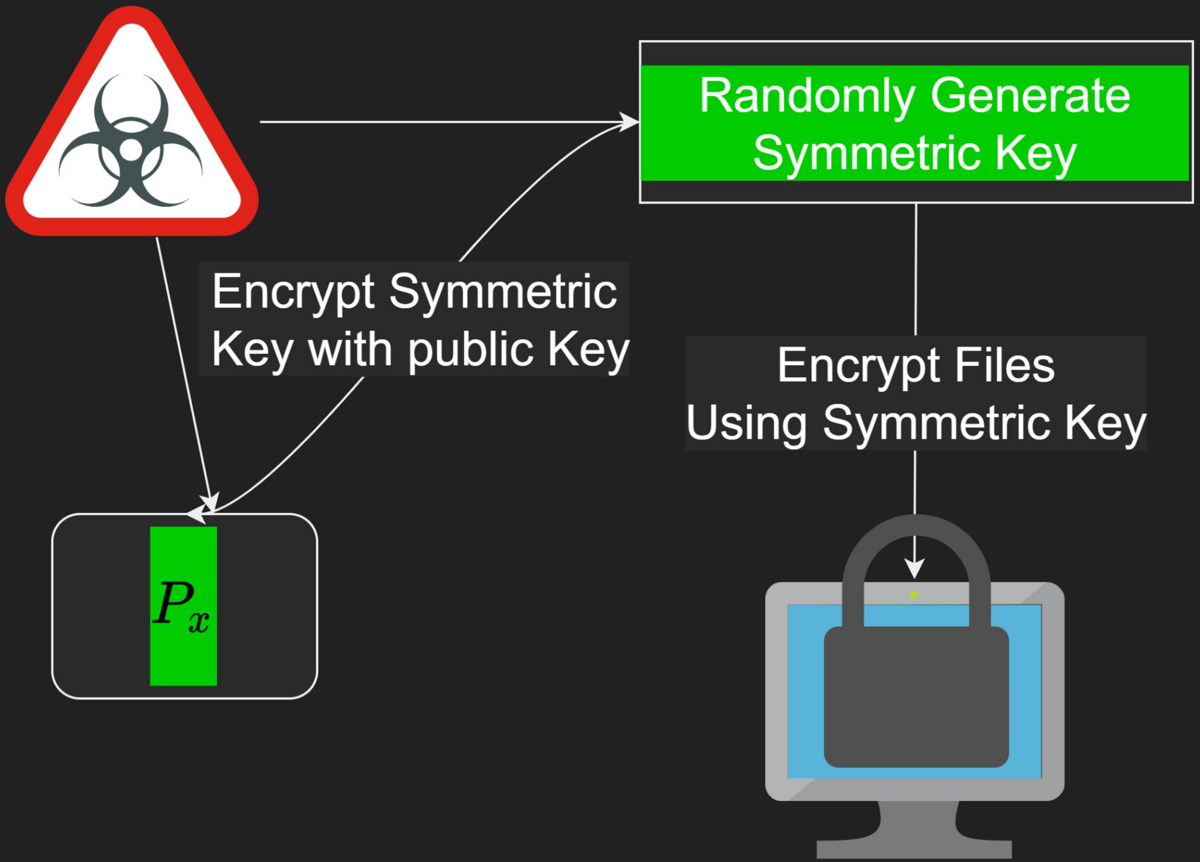
Various using Elliptic Curves

Key Agreement: Diffie Hellman

- Relied on the difficulty of the Discrete Logarithm problem in addition decisional/computational Diffie-Hellman assumption
- Easy(ish) to implement, but requires very large modulus, with very large prime factors



Ransomware


Randomly Generate Symmetric Key
Encrypt Symmetric Key with public Key
Encrypt Files Using Symmetric Key
P_x

Defeating the defenders

- Use of of public key cryptography to make key recovery impossible
- Hybrid scheme:
- Store public key on Implant
- Randomly generate a strong symmetric key
- Encrypt files using symmetric key
- Encrypt Symmetric key with public key
- “Shred” symmetric key

Common Mistakes

Key reuse (RC4, Public/Private key pairs...etc)

Small modulus (diffie Hellman)

Weak PRNG to generate symmetric keys

Key Reuse:

DarkSide Leaks Main Press Center

About Windows decryption. 12.01.2021

Bitdefender has released a utility that can decrypt some of our Windows lockers. Linux decryption is impossible.
The problem was in generating private keys in Linux. There are no encryption vulnerabilities or other problems in the locker.
Bitdefender created a decryptor that uses a private key previously purchased from us.
Due to the problem with key generation, some companies have the same keys (up to 40% of keys).
At the moment, this problem has been fixed, new companies have nothing to hope for, since the **encryption algorithms and their implementation in our locker are reliable.**
Special thanks to BitDefender for helping fix our issues. This will make us even better.

All partners who have lost profits due to this incident will receive compensation from our deposit. Now it is $ ~ 600k.

P.S.
You have chosen the wrong time to publish your decryptor, as the activity of us and our partners during the New Year holidays is the lowest. Those companies that wanted to decrypt files before the new year have already bought a decryptor, your decryptor will be useful for 2-3 companies. But now, you will never decrypt us ;)

https://www.technologyreview.com/2021/05/24/1025195/colonial-pipeline-ransomware-bitdefender/