CNS Homework2

姓名: 徐有慶
學號: r05922162

Handwriting:

1. Encryption Algorithms:

Differences:

- Symmetric cryptography 只需要一個 shared secret key 即可，Asymmetric cryptography 則需要 public 和 private key
- Shared secret key 只有要溝通的雙方可以知道，而 public key 可以被全部的人知道，private key 則只有擁有者知道

Example:

Symmetric cryptography:

- DES
- AES

Asymmetric cryptography:

- RSA
- ElGamal

To achieve higher security, which method usually needs a larger key?

Asymmetric cryptography needs a larger key

因為 Asymmetric cryptography 在 public key 的部分是公開的，若是產生方法的 key 很簡單或是 key 的長度不夠長的話，可能很容易就被別人給破解，只好靠增加 key 的大小來提升破解的難度。

Which method is generally faster, why?

Symmetric cryptography is generally faster

如上面所說，Asymmetric cryptography 需要較大的 key，計算量也相對較大，所以速度就會比較慢。

2. Three-way Diffie-Hellman

A -> B: g^a mod p

B -> C: g^{ab} mod p

C -> B: g^c mod p

B -> A: g^{bc} mod p

Shared secret key: g^{abc} mod p

3. ElGamal threshold decryption

必須假設有一個 Trusted Third Party(TTP)，在 Setup 時，會把 secret key 分配給 n 個人，在 decrytion 時，負責做解密。

Setup:

TTP 將 secret key b 用 Shamir's secret sharing 的方法分配給 n 個人(第 i 個人拿到 bi = (xi, yi))，其中至少要有 t 個人合作才能重建 secret key b，並將每個人的 public key 設成 g^yi(mod p)

Decryption:

每個人都會收到 c1 及 c2，而至少要有 t 個人計算 d_i = c1^yi (mod p)，如果 TTP 收到 t 個人回傳的 di 就可以做根據 Shamir's secret sharing 的 secret reconstruction 做解密。

Capture The Flag:

4. ECB Encryption Mode

Flag:

BALSN{W0w_y0u_4r3_r3411y_4_cu7_4nd_p4st3_m4st3r}

由 login.py 當中可以得知 ECB mode 的 block size 為 16bytes，代表每 16bytes 就會做一次 AES，而要讓系統認定為是 admin 則要在明文當中有 role=admin 出現。利用 cut-and-past-attack，先利用 username = aaaaaaaaaaaaaaaaaaa，password = b 登入，可以得到[login=aaaaaaaaaa]及[aaaaaaaaaa&role=]的 token，再利用 username = aaaaaaaaaaadmin，password = bbbbbbbbbbbb 登入，可以得到[admin&role=user&]及[pwd=bbbbbbbbbbbb]的 token，再把上述得的到 token 串接起來就可以得到 username = aaaaaaaaaaaaaaaaaaa，passwrod = bbbbbbbbbbbb 的 token 且身分為 admin，對應的明文為 login=aaaaaaaaaaaaaaaaaaa&role=admin&role=user&pwd=bbbbbbbbbbbb。

5. Beginner's RSA

(1)

Flag: BALSN{V3RYW311}

利用網站 http://www.factordb.com/對 n 做因式分解，得到 p 和 q，就能算出 d，也就可以解密。

(2)

Flag: BALSN{Forty Years of Attacks on the RSA Cryptosystem}

搜尋到已知 d、e 的話，有一個比較有效率的方式可以因式分解 n，得到 p、q，而因為 n 相同，也知道 Alice 的 public key e’，就可以得到 Alice 的 private key d’，也就可以解密。

Reference:

[1] https://goo.gl/n5zycr

(3)

Flag: BALSN{Keep calm and count prime numbers}

假設 Alice 的 public key 為 e，Bob 的 public key 為 e’，如果 gcd(e, e’) = 1 的話，存在有 s1、s2 使得 e * s1 + e’ * s2 = 1，且 $Ca = M^{e} \bmod n$，
$Cb = M^{e'} \bmod n$ 則:

$$Ca^{s1} * Cb^{s2} \bmod n = (M^{e})^{s1} * (M^{e'})^{s2} \bmod n$$

$$= M^{(e*s1)} * M^{(e'*s2)} \bmod n$$

$$= M^{(e*s1+e'*s2)} \bmod n$$

$$= M^{1} \bmod n$$

$$= M \bmod n$$

假設 s2 為負數的話，就計算 Cb 在 mod n 下的反元素 $I = Cb^{-1} \bmod n$，最終求得 $M = Ca^{s1} * I^{-s2} \bmod n$

Reference:

[1] https://goo.gl/x7KJxf

[2] https://goo.gl/JCjMhJ

6. Digital Certificate

Flag:

BALSN{b451c_s3!f_51gn3d_c3rt1fic4t3}

VALUABLE_INFORMATION{Our_boss_is_Tom!}

1. openssl genrsa -des3 -passout pass:x -out server.pass.key 2048
2. openssl rsa -passin pass:x -in server.pass.key -out server.key
3. rm server.pass.key
4. openssl req -new -key server.key -out server.csr
   輸入 hw2.pdf 上對應的資訊
5. openssl x509 -req -sha256 -days 365 -in server.csr -signkey server.key -out server.crt

做完即可拿到 certificate

Reference:

[1] https://goo.gl/uqvYIz

7. I need your help

Flag: BALSN{Now_you_know_the_secret}

從網路上得知，這種格式的 private key 可以做分解，藉此得到它的 n, e, d 等資訊，先把比較完整的那一部分做 base64 decode，轉成 16 進位後，就可以分解出它的 p、q、dP(d mod (p-1))及 dQ(d mod (q-1))，由 e=1 開始，找出對應的 d，這個 d 算出來的 dP'、dQ'要和我們分解出來的 dP、dQ 相等，不相等的話就 e+1，直到找到正確的 e 及 d。

Reference:

[1] https://goo.gl/PqIaO5
[2] https://goo.gl/5Lw9aI

8. I will look for you, and I will find you

(1)

Flag: BALSN{Don't underestimate the power of the Dark Web}

安裝完 Tor 瀏覽器連上去即可拿到 Flag