Soal

Praktikum:

- P1 (http://172.18.78.39/challenges?category=1)
- P2 (http://172.18.78.39/challenges?category=2)
- P3 (http://172.18.78.39/challenges?category=3)
- P4 (http://172.18.78.39/challenges?category=4)
- P5 (http://172.18.78.39/challenges?category=5)
- P6 (http://172.18.78.39/challenges?category=6)

1. Pangkat Modulo 1 (challenge?id=32) (1 poin) ✔

Deskripsi | Hint

Salah satu operasi dasar dalam kriptografi kunci publik adalah perpangkatan modulo. Hitunglah $17^3 \bmod 25$.

Di soal ini Anda bisa menghitung pangkatnya dahulu baru di-modulo-kan.

2. Pangkat Modulo 2 (challenge?id=33) (5 poin) ✔

Deskripsi | Hint

Hitunglah $17^{2017} \bmod 25$.

Di kasus ini sepertinya Anda tidak mungkin menghitung pangkatnya dahulu baru di-modulo-kan. Simak artikel berikut (https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/fast-modular-exponentiation) untuk mencari tahu cara menghitung pangkat modulo tanpa harus menghitung pangkatnya secara keseluruhan.

3. Pangkat Modulo 3 (challenge?id=34) (5 poin) ✔

Deskripsi | Hint

Dalam penggunaan real, misalnya dalam kriptosistem RSA, nilai yang digunakan bisa sangat besar, dalam contoh ini modulus berukuran 2048 bit.
Hitunglah (dengan komputer) hasil dari $m^e \bmod n$ dengan:

```
e = 65537
m = 94217557849073156055422415695853174106190609753661166379495
n = 21690335638476501228469645552550485684809195649973430854298
```

4. Kunci Publik RSA (challenge?id=35) (1 poin) ✔

Deskripsi | Hint

Dengan nilai $p = 3$ dan $q = 11$, tentukan kunci publik (pasangan (n,e)) jika digunakan $e = 7$.

Kunci publik dituliskan dalam format n,e dipisahkan dengan koma.

5. Kunci Privat RSA (challenge?id=36) (2 poin) ✔

Deskripsi | Hint

Dengan definisi seperti pada soal (4), tentukan kunci privat (pasangan (n,d)).

Kunci publik dituliskan dalam format n,d dipisahkan dengan koma.

6. Enkripsi RSA (challenge?id=37) (1 poin) ✔

Deskripsi | Hint

Dengan parameter kunci publik seperti soal (4), enkripsikan pesan $m = 14$.

7. Dekripsi RSA (challenge?id=38) (1 poin) ✔

Deskripsi | Hint

Dengan parameter kunci privat seperti soal (5), dekripsikan ciphertext \(c = 14\)

8. Representasi Data 1 (challenge?id=39) (1 poin) ✔

Deskripsi | Hint

Algoritme kunci publik bekerja dalam aritmatika bilangan, sedangkan data digital berupa deretan byte. Bagaimana caranya supaya deretan byte itu bisa dioperasikan dengan operasi bilangan?

Caranya adalah dengan mengubah deretan byte tersebut menjadi bentuk hexadecimal (encode ke hexadecimal), kemudian dari hexadecimal diubah menjadi desimal.

Cobalah tentukan bagaimana representasi string "ILKOM" menjadi angka.

8.5. Batasan (challenge?id=43) (1 poin) ✔

Deskripsi | Hint

Salah satu konsekuensi operasi bilangan modulo pada RSA adalah bahwa pesan yang akan dienkripsi besarnya tidak boleh melebihi modulus (\(n\)) supaya bisa didekripsi dengan benar. Tentukanlah apakah pesan "tidaaaaak" dapat dienkripsi dengan nilai modulus \(n = 14880885840517412773\).

Jawab "ya" atau "tidak". Anda hanya boleh menjawab 1 kali.

9. Representasi Data 2 (challenge?id=40) (1 poin) ✔

Deskripsi | Hint

Sekarang adalah proses kebalikan dari soal (8). Ubah angka berikut (desimal) menjadi string kembali: 5395265.

Note: jika bentuk hexadecimal-nya memiliki jumlah digit ganjil, tambahkan 0 di depan.

10. Format PEM 1 (challenge?id=41) (2 poin) ✔

Deskripsi | Hint

Kunci publik maupun private RSA biasanya disimpan dalam file dengan format PEM (https://en.wikipedia.org/wiki/Privacy-enhanced_Electronic_Mail). Format PEM dapat dibuat misalnya dengan beberapa baris kode Python berikut:

```
n = ... # modulus
e = ... # public exponent
d = ... # private exponent

from Crypto.PublicKey import RSA
key = RSA.construct((long(n), long(e), long(d)))
print(key.exportKey('PEM'))
```

Buatlah format PEM untuk key dengan $n = 24493441176670225263814235378142462670 9$, $e = 65537$, dan $d = 326942983983873431161612704726557393 93$.

11. Format PEM 2 (challenge?id=42) (2 poin) ✔

Deskripsi | Hint

Tentukan nilai n dari public key dalam format PEM berikut:

```
-----BEGIN PUBLIC KEY-----
MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgGzjwzBuWBfyHgmMqMkvtIIFIsv
xXKic+cbe5RleWSOkYMp5QePKk8QKTwu3+zSN4kJk/eO3N/rJQ1ln0Zxy/wt/tX
neFjer3rpZXW9Sf7XvFG47J3AqJTjF1vlELz5/reHHReZ0CO7ZXk9ilVETqg879
lLHs+lDMAt7EuvjDAgMBAAE=
-----END PUBLIC KEY-----
```

Hint: dapat diambil nilainya dengan beberapa baris kode Python berikut:

```
pem = '...' # string format PEM

from Crypto.PublicKey import RSA
pubkey = RSA.importKey(pem)

print(pubkey.n)
print(pubkey.e)
```

12. Komunikasi RSA 1 (challenge?id=44) (5 poin) ✔

Deskripsi | Hint

Pada zaman dahulu ada dua sahabat yaitu Asep dan Bejo. Mereka akan berkomunikasi secara aman dengan memanfaatkan konsep kunci publik RSA. Mereka memilih kriptografi kunci publik karena mereka berdua tidak ingin bertukar kunci secara rahasia.

Kedua belah pihak memiliki kunci publik dan kunci privat masing-masing. Kunci publik masing-masing diberikan kepada temannya (Asep memiliki kunci publik Bejo, dan Bejo memiliki kunci publik Asep), sementara kunci privat disimpan masing-masing (namanya juga kunci privat). Seluruh kunci yang digunakan terlampir pada soal ini.

Alkisah Asep ingin mengirim pesan kepada Bejo: "pinjem duit dong". Tentukan ciphertext apa yang dikirimkan oleh Asep kepada Bejo setelah dienkripsi dengan RSA. Tuliskan hasil dalam hexadecimal.

Hint: Kalau Asep mengirim ke Bejo, yang digunakan kunci publik atau privat, dan kunci milik siapa yang digunakan?

Download:

kunci_rsa.zip (download?file_key=9a9443e412fd0f4caaf62fa54207b3881c0d225c26e86640cef5e556631d31a8&team_key=7a2f2380fabc3520adf57294ee291bdec2c04101383b2e6433abac3d7353c213) (2.23 KB)

13. Komunikasi RSA 2 (challenge?id=45) (7 poin) ✔

Deskripsi | Hint

Soal ini menggunakan kunci dan deskripsi kedua pihak seperti soal (12). Alkisah lagi, kemudian Bejo membalas pesan Asep seperti berikut (sudah terenkripsi RSA dan di-encode dalam hexadecimal):

```
576ad6cc63327540d80729f343d5e68349dd104f2bb40552bd4896b5d8ed80a
```

Tentukan pesan apakah yang dikirimkan Bejo kepada Asep!

14. Break Weak RSA (challenge?id=46) (10 poin) ✔

Deskripsi | Hint

Kekuatan algoritme RSA bertumpu pada pada sulitnya memfaktorkan modulus (\(n\))

menjadi 2 bilangan prima penyusunnya. Jika modulus berhasil difaktorkan, maka keamanannya sudah bobol. Karena itulah biasanya nilai (\(n\)) dibuat sangat besar, biasanya 1024 atau 2048 bit.

Di soal ini dicontohkan kunci publik RSA yang lemah, hanya 64 bit. Diketahui kunci publik \((n,e) = (7645419950178196741,17)\). Kunci tersebut digunakan untuk mengenkripsi suatu pesan rahasia menjadi \(c = 1859633570218459779\) (dalam desimal). Tentukan pesan tersebut (berupa string).

Copyleft 2015
Cyber Security IPB (https://www.facebook.com/cysecipb)