

ورقات بيضاء في المختبر

WHITE PAPERS in ViTRO

(06/2020) #04



سلسلة

نظرة و تجربة

موضوع اليوم

RSA 1024 (ACHILLES' HEEL)



ينتاب المهندس العكسي الشعور بالإحباط عندما يصـادف إشكالات تلمس
التشفير، خصوصا خوارزميات التشفير القوية و الصعبة، و منبع هذا الشعور
هو ما يتم تداوله عن قوتها و استحالة كسرها او ما تحتاجه من موارد و زمن
خيالي لحلها.

طبعا ما يتم تداوله عنها صحيح الا ان هناك جزء من المهم ان نتطرق اليه، و
هو الثغرات و الضعف الذي تعاني منه بعض المفاتيح التي تعتبر قوية مثل
مفتاح تشفير **RSA** بطول **1024** موضوع هذه الورقة البيضاء.

قصة الشخصية الأسطورية المعروفة باسم اخيليس و كعبه ACHILLES' HEEL:

كان هذا الأخير من اقوى المحاربين في وقته الا ان سبب موته هو ضربة رمح اصابته
كعبه تسببت في عجزه و من ثم مقتله، و نتجت عن ذلك مقولة مشهورة يوصف بها
الشيء القوي المصاب بضعف يؤدي الى انهياره التام.

RSA التشفير القوى المرعب:

التشفير RSA مبني على آلية توليد مفاتيح **مختلفين** (PUBLIC/PRIVATE) يدخلان في عملية التشفير وفك التشفير (ASYMMETRIC) مع إمكانية التحكم في طول المفاتيح المولدة، كلما كان طول المفتاح كبير ضلّت إمكانية كسره.

التمرين:

هو كلمة تم تشفيرها بمفتاح **RSA** عام **PUBLIC** بطول **1024** متاح و ظاهر للجميع:

الكلمة المشفرة:

```
ciphertext =  
937FC27E08B3557B989D98197EBCBA8A983A750AEC00A4E55DA6DA08ABD7D733  
48CD24AF55D93E3D9229594135704425D4850C74AC978B8CFD0C4D6508463634  
5940E36BA4A3AD784AFC1B685B26212ED152B059B2DA2A7F0296E7FED9E532A9  
23C858E6B98E9013D354709F7DE6C7B54950F17FF5692B9AA799E266496DFA30
```

```
S3C828EEB8E80T3D324J08EJDEECJB24820LTJLE2e8SB8VWJ88ESee48eDEY30  
2840E3eBY4Y3YD184YLCJBe82BSesTSEDt23B028BSDV3YJLO38eEJLED8E233Y8  
48CD34WLE22D83E3D83S8284T32J044S2D4820CJ4WC8J8B8CELD0C4D8e2084e3e34  
83JEC3JE08B322JB888D88T8JEBCB8V8V883YJ20VEC00V4E22DV8DV08VBDJJD33
```

المفتاح العام **N** :

```
n=  
9BE29093439A7855DFF27D74C7BCAC60FECA520AE10F82EB7493BEE6D100C501  
C0D10088593098FCBFD476B2F3EA27961AB362076F3640B91B761CD664A5115D  
38C391D6671CE9E0E1C05785A85C477F171FE3B32359D74F599A46381974D20A  
5C6F873C2FCDA0BB0A5730C5D3925FA1FF2FA8D7FDDBBF84F860D5531EADB66D
```

```
2C8E8J3CSLECDV0BB0V2J30C2D38S2EYTELES8V8DJEDDBBE84E8e0D223TEVDBeED  
38C38TDe8JTCe8E0ETC02J82V82C4JJLEJAJTEE3B3S328DJ4E288V4e38T8JJDS0V  
C0DT0088283088ECB8D4JEBSE3EY3J8eTWB3eS0J8E3e40B8TBJ8TCDe84W2JT2D  
8BE38083438VJ822DELSJJDJ4CJBCVCE0EECY230VET0E8SEBJ483BEEDT00C20T
```

قيمة **E** تركت افتراضية:

```
e=  
10001
```

```
T000T  
6=
```

من المفروض ان اتاحة ونشر المفتاح "العام" بطول 1024 يعطينا نوعا ما (ضمان) في الوقت الحالي بعدم إمكانية كسره و الحصول على المفتاح "الخاص" الذي يعطي لمالكه إمكانية فك التشفير...

الا ان المفتاح (العام) للتمرين مصاب بضعف في (كعبه) يتيح الحصول على المفتاح "الخاص" في اقل من ثانية.

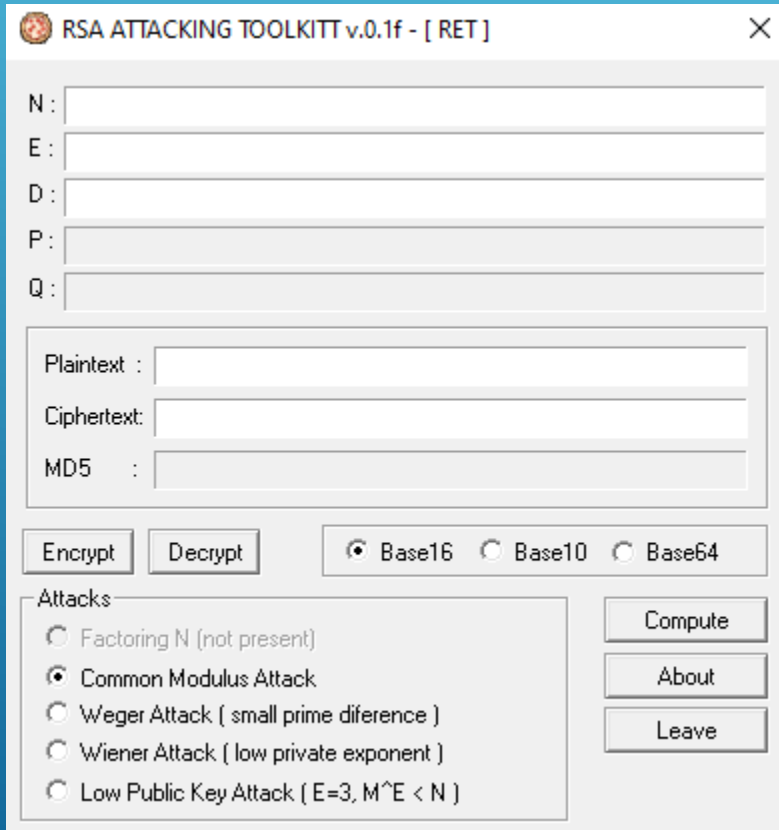
عملية كسر المفتاح "العام" و الحصول على المفتاح "الخاص" :

للتعامل مع مفاتيح **RSA** تم التوجه لتجربة "الهجمات" المنشورة على النت، و بسبب طول مفتاح

التمرين **1024** تعذر اتباع منهج **FACTORIZATION** و التركيز على الهجمات التي تلمس نقط

ضعف معينة.

و اعتمادا في ذلك على أداة **RSA ATTACKING TOOLKIT**



RSA ATTACKING TOOLKIT v.0.1f - [RET]

N :

E :

D :

P :

Q :

Plaintext :

Ciphertext:

MD5 :

Encrypt Decrypt ☒ Base16 ☐ Base10 ☐ Base64

Attacks

☐ Factoring N (not present)

☒ Common Modulus Attack

☐ Weger Attack (small prime difference)

☐ Wiener Attack (low private exponent)

☐ Low Public Key Attack ($E=3, M^E < N$)

Compute

About

Leave

RSA ATTACKING TOOLKIT v.0.1f - [RET]

N : 9BE29093439A7855DFF27D74C7BCAC60FECA520AE10F82EB7493BEE

E : 10001

D :

P :

Q :

Plaintext :

Ciphertext:

MD5 :

Encrypt Decrypt Base16 Base10 Base64

Attacks

☐ Factoring N (not present)

☐ Common Modulus Attack

☒ Weger Attack (small prime diference)

☐ Wiener Attack (low private exponent)

☐ Low Public Key Attack ($E=3, M^E < N$)

Compute About Leave

تجربة الهجوم المسمى WEGER

01 - ادخال المفتاح "العام" N

02 - ادخال القيمة الافتراضية E

03 - تفعيل خيار WEGER ATTACK

04 - وأخيرا النقر على الزر COMPUTE

RSA ATTACKING TOOLKIT v.0.1f - [RET]

N : 9BE29093439A7855DFF27D74C7BCAC60FECA520AE10F82EB7493BEE

E : 10001

D : 2625CDC79C15A33930B2C0ECE12C54EAEFAF47608E2F2394C75498B

P : C7C42A9E37786E981D9F58A16FB17EF082F588903B49D3F51E63B28E

Q : C7C42A9E37786E981D9F58A16FB17EF082F588903B49D3F51E63B28E

Plaintext :

Ciphertext:

MD5 :

Encrypt Decrypt

Base16 Base10 Base64

Attacks

☐ Factoring N (not present)

☐ Common Modulus Attack

☒ Weger Attack (small prime difference)

☐ Wiener Attack (low private exponent)

☐ Low Public Key Attack ($E=3, M^E < N$)

Compute

About

Leave

بعد النقر على زر **COMPUTE** نلاحظ انه تم الحصول

في اقل من ثانية على المفتاح "الخاص" **D** وقيم الـ **PRIMES (P/Q)**

```
d=
2625CDC79C15A33930B2C0ECE12C54EAEFAF47608E2F2394C75498B517949EA1
8D341873459055001559C32A8BF25379B2530FBC4E04F2D5D9D88FBA0FAB2D92
46D9CE3CC7B4CFEE32F12B64D095E0E423C5CF7A4179C6837208513E6D9A4E3C
42D26D59C62D8D040F7327D0A5F285F13570A098B4664E13EDF3C2296A4FCC69

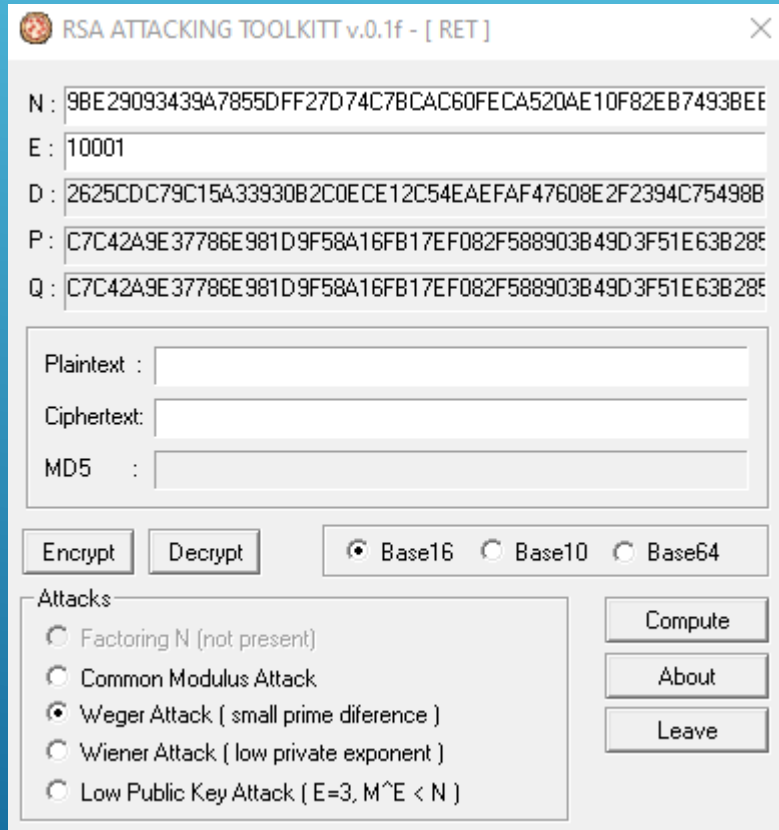
p=
C7C42A9E37786E981D9F58A16FB17EF082F588903B49D3F51E63B285E3388B41
202E8136B1D86C2CA3FBBF2D004B646B3D5FFB2A3347C23ABA64B5BB235B9F5C7

q=
C7C42A9E37786E981D9F58A16FB17EF082F588903B49D3F51E63B285E3388B41
202E8136B1D86C2CA3FBBF2D00FE7316A68E649429009018D96A5C1477CB222B
```

التفسير:

خلال اول مرحلة توليد المفاتيح الخاصة ، العامة وقيم "البرايمز"

نتج تقارب كبير في قيم "البرايمز" P و Q



```
p=
C7C42A9E37786E981D9F58A16FB17EF082F588903B49D3F51E63B285E3388B41
202E8136B1D86C2CA3FBBF2D04B646B3D5FFB2A3347C23ABA64B5BB235B9F5C7

q=
C7C42A9E37786E981D9F58A16FB17EF082F588903B49D3F51E63B285E3388B41
202E8136B1D86C2CA3FBBF2D00FE7316A68E649429009018D96A5C1477CB222B
```

هذا التقارب اصبح "كعب اخيليس"، وباستعمال أدوات مثل RAT

التي تدعم هجوم تقارب قيم "البرايمز" امكنا الحصول على المفتاح

الخاص PRIVATE KEY (D)

```
d=
2625CDC79C15A33930B2C0ECE12C54EAEFAF47608E2F2394C75498B517949EA1
8D341873459055001559C32A8BF25379B2530FBC4E04F2D5D9D88FBA0FAB2D92
46D9CE3CC7B4CFEE32F12B64D095E0E423C5CF7A4179C6837208513E6D9A4E3C
42D26D59C62D8D040F7327D0A5F285F13570A098B4664E13EDF3C2296A4FCC69
```

RAT – RSA ATTACKING TOOL

عملية فك التشفير:

حسب المتفق عليه في طريقة استعمال الـ **RSA** فإن:

- التشفير يتم باستعمال **N** و **E** فقط.
- فك التشفير يتم باستعمال **N** و **D** فقط.



نتائج الصور للعملية الخاصة بالتمرين:

```
d=
2625CDC79C15A33930B2C0ECE12C54EAEFAF47608E2F2394C75498B517949EA1
8D341873459055001559C32A8BF25379B2530FBC4E04F2D5D9D88FBA0FAB2D92
46D9CE3CC7B4CFEE32F12B64D095E0E423C5CF7A4179C6837208513E6D9A4E3C
42D26D59C62D8D040F7327D0A5F285F13570A098B4664E13EDF3C2296A4FCC69

p=
C7C42A9E37786E981D9F58A16FB17EF082F588903B49D3F51E63B285E3388B41
202E8136B1D86C2CA3FBBF2D04B646B3D5FFB2A3347C23ABA64B5BB235B9F5C7

q=
C7C42A9E37786E981D9F58A16FB17EF082F588903B49D3F51E63B285E3388B41
202E8136B1D86C2CA3FBBF2D00FE7316A68E649429009018D96A5C1477CB222B

plaintext =
[www.at4re.net]

ciphertext =
937FC27E08B3557B989D98197EBCBA8A983A750AEC00A4E55DA6DA08ABD7D733
48CD24AF55D93E3D9229594135704425D4850C74AC978B8CFD0C4D6508463634
5940E36BA4A3AD784AFC1B685B26212ED152B059B2DA2A7F0296E7FED9E532A9
23C858E6B98E9013D354709F7DE6C7B54950F17FF5692B9AA799E266496DFA30
```

RSA ATTACKING TOOLKIT v.0.1f - [RET]

N : 9BE29093439A7855DFF27D74C7BCAC60FEC4520AE10F82EB7493BEE

E : 10001

D : 2625CDC79C15A33930B2C0ECE12C54EAEFAF47608E2F2394C75498B

P : C7C42A9E37786E981D9F58A16FB17EF082F588903B49D3F51E63B285

Q : C7C42A9E37786E981D9F58A16FB17EF082F588903B49D3F51E63B285

Plaintext : [www.at4re.net]

Ciphertext: 937FC27E08B3557B989D98197EBCBA8A983A750AEC00A4E55DA6DA08ABD7D73348CD24AF55D93E3D9229594135704425D4850C74AC978B8CFD0C4D65084636345940E36BA4A3AD784AFC1B685B26212ED152B059B2DA2A7F0296E7FED9E532A923C858E6B98E9013D354709F7DE6C7B54950F17FF5692B9AA799E266496DFA30

MD5 : DD44D9D2855256ACE26D7924BEE41ED2

Encrypt Decrypt Base16 Base10 Base64

Attacks

- ☐ Factoring N (not present)
- ☐ Common Modulus Attack
- ☒ Weger Attack (small prime difference)
- ☐ Wiener Attack (low private exponent)
- ☐ Low Public Key Attack ($E=3, M^E < N$)

Compute About Leave