FORSVARETS EFTERRETNINGSTJENESTE

Løsning til kryptokampagnen 2023

Kampagnen bestod af tre elementer; sociale medier, et medarbejderportræt og et stillingsopslag. Opgaver og hints var fordelt på alle tre elementer.

1) Sociale medier

```
Ymzj ul yri silx wfi yarvcg jrr yri Alczv efxcv yzekj.
```

Et simpelt substitutionsciffer (blokke af forskellig længde).
Cæsarciffer som skiftes 9 pladser giver:

```
Hvis du har brug for hjaelp saa har Julie nogle hints.
```

Dette er en reference til **Mød en krypto-profil** medarbejderportrættet (side 5)

Ovenstående billeder fra sociale medier gemmer den samme opgave og de samme hints:

Første del af opgaven	$N = 322^{129} + 1333^{15}$ $e = 2^{16} + 1$ $key = 1337^{d} \bmod N$ $key \% 0xfe = 204$
Anden del af opgaven	`m = decrypt(sha256("%d" % key), c)`
Hint til første del af opgaven	`rsa`

Hints til anden del af opgaven	`stream`
	`0x00*8`
	`count=0`

Første del af opgaven
Hintet siger RSA hvilket stemmer overens med de viste beregninger. I RSA ligger sikkerheden i, at det er svært at faktorisere et produkt af to store primtal.

Billedet med opgaven giver en offentlig nøgle bestående af N og e. For at finde key er det nødvendigt at finde den private RSA-nøgle d.

Da vi har med RSA at gøre, ved vi, at N kan udtrykkes som N = p*q, hvor p og q er primtal. Det er velkendt, at den private nøgle d kan konstrueres ud fra disse p og q. I denne opgave er N valgt på en sådan måde, at faktoriseringen kan indses direkte. Måske lagde du mærke til, at primtallet 3 går op i eksponenterne 129 og 15, som kunne give en mistanke til en teleskop-agtig faktorisering. Ellers gav klarteksten fra cæsarcifferet et hint til at undersøge **Mød en krypto-profil**. I slutningen af det medarbejderportræt er der en tekst, som ud fra det anvendte alfabet (der ses store og små bogstaver samt det slutter med lighedstegn) sandsynligvis er en base64 tekst. Ved at bruge fx "From Base64" i værktøjet CyberChef fås:

```
Hvis du ser tallet som et polynomium kan formlen x^129 + y^15 =
(x^43 + y^5)(x^86 - y^5 * x^43 + y^10) måske bruges?
```

Skrevet på en mere letlæselig form er ligningen:

$$x^{129} + y^{15} = (x^{43} + y^5)(x^{86} - y^5 * x^{43} + y^{10})$$

Hvis x = 322 og y = 1333 indsættes i ligningen, haves N på venstre side og en faktorisering af N på højre side:

$$N = p * q$$

$$322^{129} + 1333^{15} = (322^{43} + 1333^5)(322^{86} - 1333^5 * 322^{43} + 1333^{10})$$

Hvis den første del af højre side vælges som p og den anden som q haves:

$$322^{129} + 1333^{15} = (322^{43} + 1333^5)(322^{86} - 1333^5 * 322^{43} + 1333^{10})$$

$$p = 322^{43} + 1333^5$$

p =
688339168571559064510890633409023118072556068415553307947521668819820261272348172120258590996493624996917541

$$q = 322^{86} - 1333^5 * 322^{43} + 1333^{10}$$

q =
473810810989785206183249335304084394309924019877922194181460660379414549164923233586166841085016532206298905214099916489998878755064839730080183959658954277362706718659083359101267500159088948862882849028267625721689

Nu kan d også kaldet den hemmelige eksponent beregnes. Først skal φ(N) bestemmes, hvor φ er Eulers phi-funktion. Da p og q er primtal, er:

$$\varphi(N) = (p-1) * (q-1)$$

Herefter findes d, der for at kunne dekryptere en ciffertekst krypteret med e, skal opfylde

$$d = e^{-1} \bmod \varphi(N)$$

d der opfylder dette findes med Euklids udvidede algoritme, fx xgcd funktionen i Sagemath.

d =
186348681530906948019265318109958378607829488800238514678793711415332458572694130460867
968532815353342025199632578145306458884396154982710031514367849768256806650567637729269
176741042738355276077795431693363836974879730319148338633611456761764112318943561028105
710166652592688088385604259201789187628214649730054974253357633

Opløftes ciffertekst 1337 i d mod N fås key

key = $1337^{d} \bmod N$

key =
227857446649348275215647624464987241545636391362023478013040699386815734626065451408037
899136441568883745828351958633840245091058087960398324909397690679101231208181603855993
607345719742780245362918121267992945532766628775198487738065139866725489690423370740983
880047037716138970499389202696990105294543663986620847650920138

Som en hjælp til at verificere at den korrekte nøgle er fundet, er det givet at nøglen modulo 0xfe (254 i decimal) er 204. Dvs.:

227857446649348275215647624464987241545636391362023478013040699386815734626065451408037
899136441568883745828351958633840245091058087960398324909397690679101231208181603855993
607345719742780245362918121267992945532766628775198487738065139866725489690423370740983
880047037716138970499389202696990105294543663986620847650920138 **%** 254 = 204

Anden del af opgaven

```
m = decrypt(sha256("%d" % key), c)
```

Her skal klarteksten m findes ved at bruge den nu fundne nøgle **key** på ciffertekst **c**. **c** findes i **stillingsopslaget** (side 7).

```
c =
d7a7e396df976cf6c59adce5d1381ea020a35af126efd0d5d380e4ccb74758e0f05e86a0bed61ac75d5a1df
d029c8792ced99c5abf33354505e288f0b9bda280c9099506be3c3ee818b5e405e1fbf45903708cd067cafa
34aa5f5b88958ae6603b4a427ab2
```

Næste trin er at finde den krypteringsalgoritme der skal bruges (**decrypt**). De hints der er til denne del af opgaven peger i retning af et stream-cipher, hvilket stemmer overens med at **c** er har en længde på 101 bytes (2 hexadecimale tegn per byte; første byte er d7, anden byte er a7, e3 osv.). Havde det været et block-cipher, ville længden på ciffertekst typisk være delelig med blokstørrelsen, hvilket typisk er et multiplum af 8 bytes.

De to andre hints (0x00*8 og count=0) er inputs til det stream-cipher. Man kan ud fra dette lave nogle kvalificerede gæt på hvilke algoritmer det kunne være og prøve dem af.

Der er også et hint i **Mød en krypto-profil**, hvor Julie fortæller om en kollega, der har danset salsa i 20 år, hvilket er en reference til **Salsa20**. Ved at finde en implementering af Salsa20 og bruge den med key, IV=0x00*8 og count=0 findes m.

```
m = Salsa20(sha256("%d" % key), c)
```

```
m = Godt klaret! Hvis du har mod på mere, så send os en ansøgning. Vi glæder os
til at høre fra dig.
```

FORSVARETS EFTERRETNINGSTJENESTE

2) Mød en krypto-profil

Julie har altid beskæftiget sig med forskning, men det var en helt ny måde at forske på, da hun kom til Forsvarets Efterretningstjeneste. Her er hendes koder og algoritmer nemlig med til at gøre en direkte forskel for Danmarks sikkerhed.

"For mig har grundforskning altid fyldt meget. Jeg har en baggrund inden for naturvidenskab, og efter det har jeg arbejdet på et universitet. Men en dag dukkede der et stillingsopslag op fra FE, som åbnede mine øjne for en ny form for forskning – forskning som har en direkte effekt, og som gør en direkte forskel for Danmarks sikkerhed".

En medarbejder i FE's krypto-enhed er sjældent fuldt færdiguddannet til stillingen fra dag ét. Alle har meget forskellige profiler, og uddannelsesmulighederne spænder bredt.

"Da jeg startede i FE's krypto-enhed, havde jeg aldrig haft et kursus i kryptologi. Derfor har min læringskurve været utrolig stejl. Der var en masse nye ting at lære inden for området, men min naturvidenskabelige baggrund har været et godt afsæt til at sætte mig ind i de dele af kryptologien, jeg indtil videre har beskæftiget mig med.

Arbejdet i FE både udfordrer og udvikler mig fagligt. Der er en god stemning på kontoret, og man kan altid spørge sine kollegaer, hvis man har brug for hjælp med noget – uanset om det arbejdsrelateret eller ej. Der er nemlig også plads til andet og mere end det faglige. Bl.a. hyggelige frokostpauser med snakke om fritidsinteresser, som spænder bredt fra outdooraktiviteter til ***salsa på 20ende år***".

I krypto-enheden er der mange forskelligartede opgaver – en del af dem er projektorienterede og indebærer ofte identificering af mønstre i data, der kan udnyttes til kryptoanalyse eller optimering af modeller.

"Normalt bruger jeg det meste af min tid på at udvikle machine learning-modeller, men mit nuværende projekt er inden for et helt andet felt. Projektet omhandler nemlig optimering og videreudvikling af en algoritme til afvikling på et HPC-system. Jeg har blandt andet arbejdet med at få vores maskinkode på vores HPC til at køre hurtigere, så vi kan udnytte vores beregningskraft mere effektivt. Som minimum får vi kørt vores beregninger billigere, hvilket giver plads til flere nye projekter, og ideelt gør det, at vi kan løse ting, vi ikke kunne før. Det kan skabe helt nye kapaciteter, der kan bidrage til FE's indhentning.

Så jeg har i FE både fået spændende opgaver inden for matematik/programmering, og et job som giver mening for mig, fordi jeg kan være med til at skabe et mere sikkert Danmark".

Forsvarets Efterretningstjeneste er en lukket verden, og derfor havde Julie, ligesom mange andre, gjort sig en masse forestillinger, inden hun startede:

"Modsat mine forestillinger om FE så er der en enorm medarbejderdiversitet. Jeg havde troet, at størstedelen af de ansatte i Forsvarets Efterretningstjeneste havde en militær baggrund, men der tog jeg grueligt fejl. Faktisk er de fleste civile, som kommer med et hav af forskellige baggrunde. Når man kommer fra en forskningsmæssig baggrund, kan det nogle gange være svært at oversætte sine kompetencer til arbejdsmarkedet udenfor universiteterne, men fordi der er så mange med en utraditionel baggrund i FE, så er der en stærk kultur for at se muligheder i folks forskelligheder og få bragt dem i spil.

*Trods forskelligheder samarbejder vi alle om et fælles mål, og hver dag møder jeg masser af hjælpsomme kollegaer, som er med til at skabe en bedre og mere sikker verde*n".

SHZpcyBkdSBzZXIgdGFsbGV0IHNvbSBldCBwb2x5bm9taXVtIGthbiBmb3JtbGVuIHheMTI5ICsgeV4xNSA9ICh4XjQzICsgeV41KSh4Xjg2IC0geV41ICogeF40MyArIHleMTApIG3lc2tlIGJydWdlcz8=

FORSVARETS
EFTERRETNINGSTJENESTE

3) Stillingsopslaget

Kryptoprofiler

Er du også interesseret i hvordan man får mest mulig performance ud af en supercomputer? Eller er du skarp til at finde nålen i den kryptologiske hø-stack? Eller kan du bare godt lide at skille ting ad? Så er vores krypto-enhed nok noget for dig.

Vores krypto-enhed vokser og vi søger krypto-kyndige folk til flere forskellige stillinger! Krypto-enheden arbejder bredt i hele FE, hvor vores særlige kompetencer og ressourcer kommer i spil i forhold til efterretningsarbejde, operationer og rådgivning.

Hvis du kan se dig selv i én eller flere af de 3 krypto-profiler hører vi meget gerne fra dig!

...

```
c =
d7a7e396df976cf6c59adce5d1381ea020a35af126efd0d5d380e4ccb747
58e0f05e86a0bed61ac75d5a1dfd029c8792ced99c5abf33354505e288f0
b9bda280c9099506be3c3ee818b5e405e1fbf45903708cd067cafa34aa5f
5b88958ae6603b4a427ab2
```