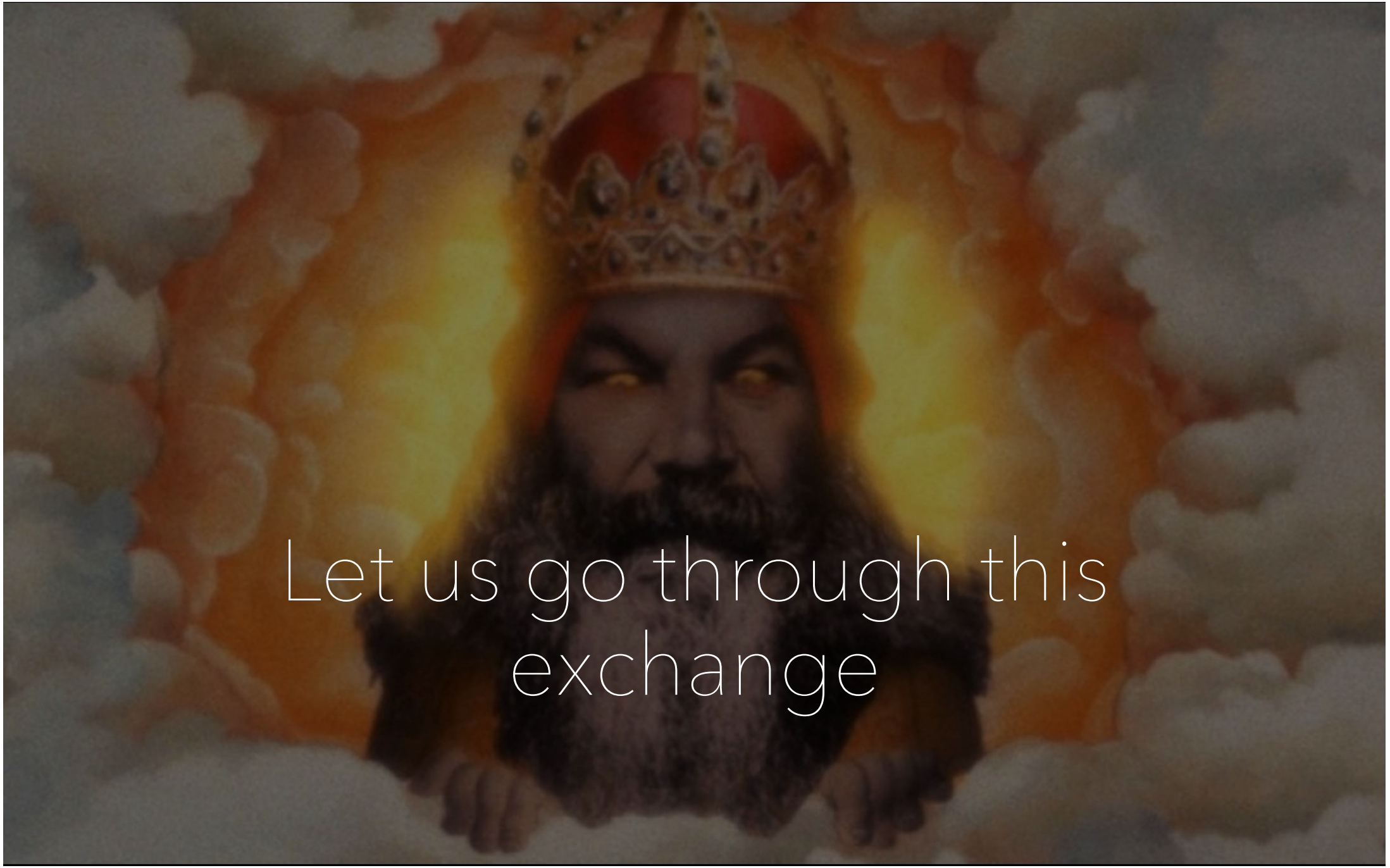
Assless Chaps: a novel combination of prior work to crack MSCHAPv2, fast

(or why MSCHAPv2 doesn't cover it's ass)

by Michael Kruger @_cablethief
& Dominic White @singe

Orange Cyberdefense's SensePost Team


hackers
industry
MSCHAPv2
No, that's not dead.
It's resting.


Let us go through this
exchange

username

I am King Arthur

authenticator challenge

I challenge you!

peer challenge

I challenge you back!

NT response

I??ۂS???^?پQ?e4L??

```
Challenge = ChallengeHash(PeerChallenge, AuthenticatorChallenge, UserName)
NTResponse = ChallengeResponse(Challenge, PasswordHash)
```

My swallow knowledge is beyond reproach!

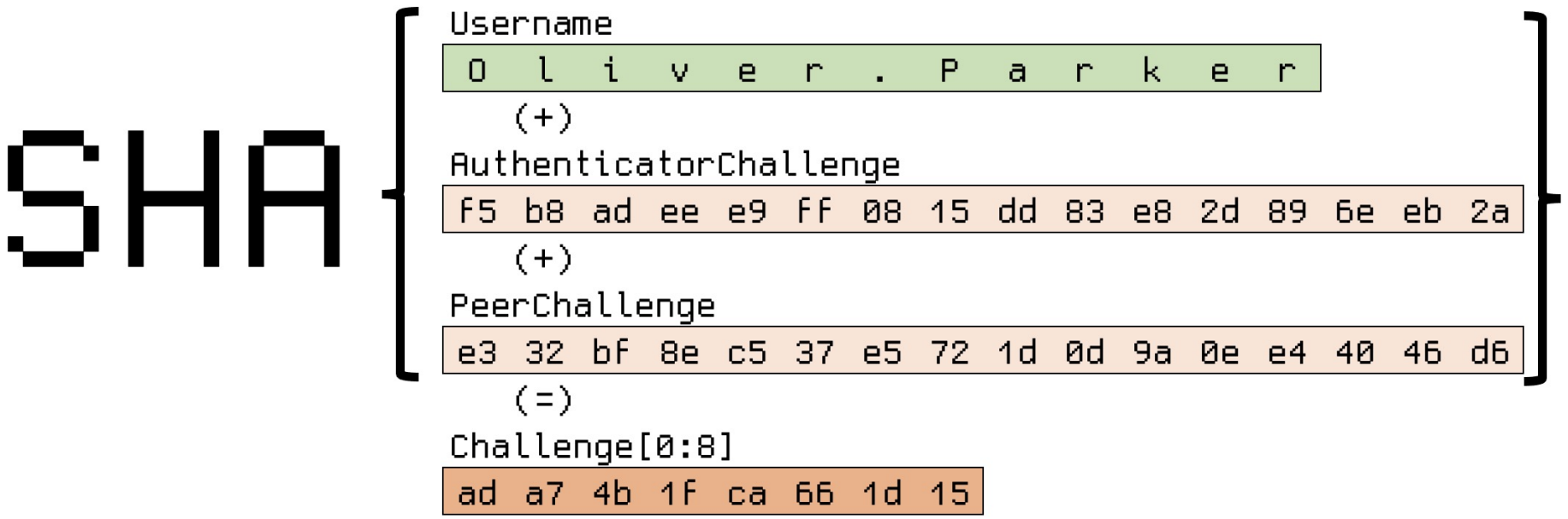
authenticator response

,`P<C{ 'K寫^pu6

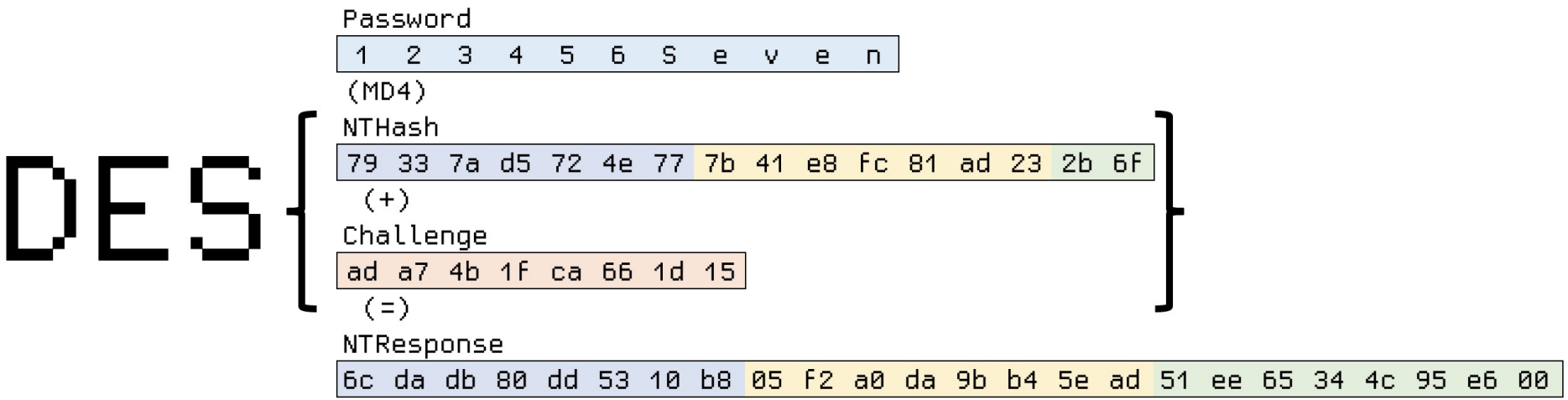
```
AuthenticatorResponse = GenerateAuthenticatorResponse(PasswordHashHash,
                        ChallengeHash, NTResponse)
Success (S=)
```


F

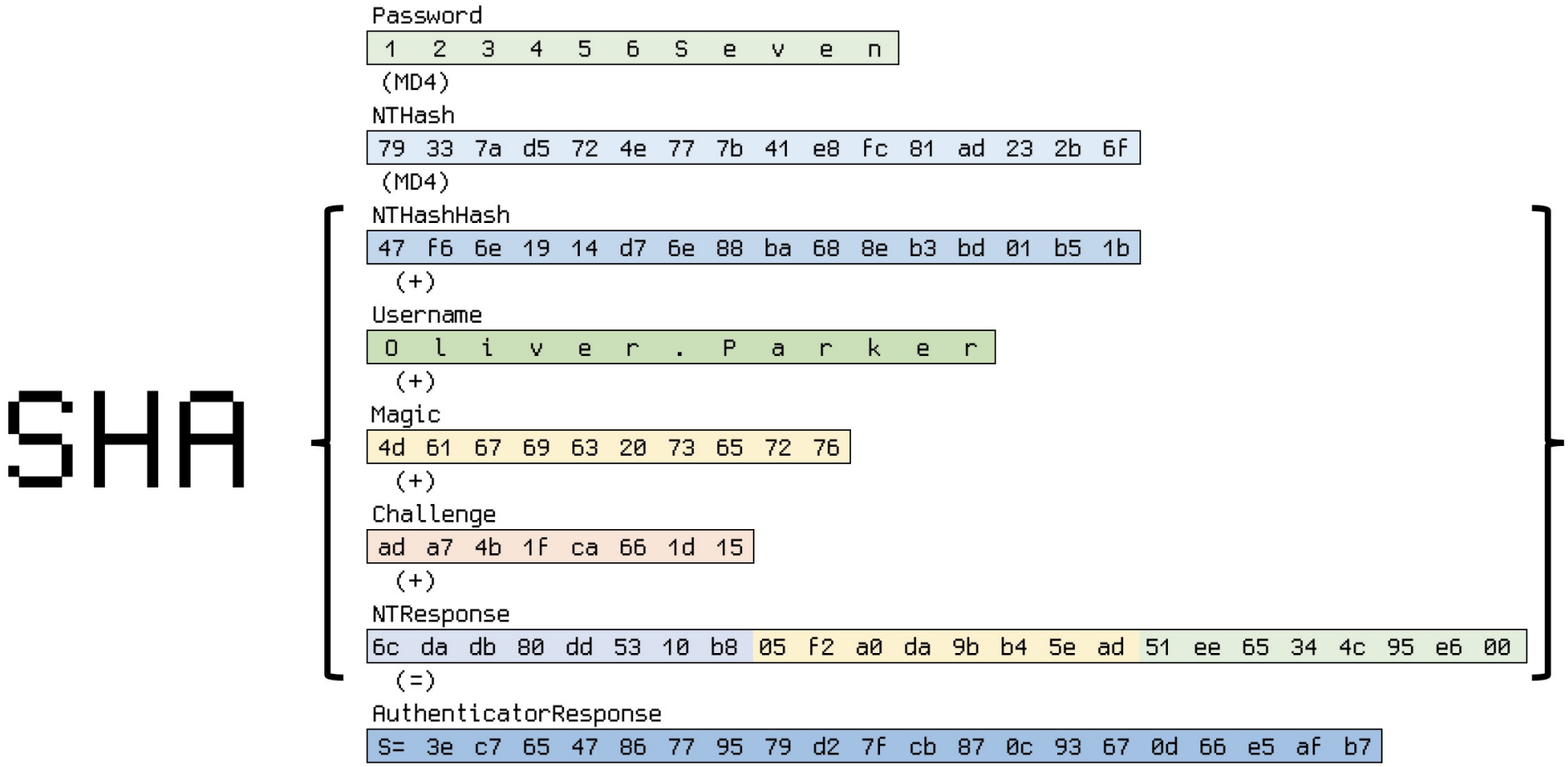
Challenge Generation



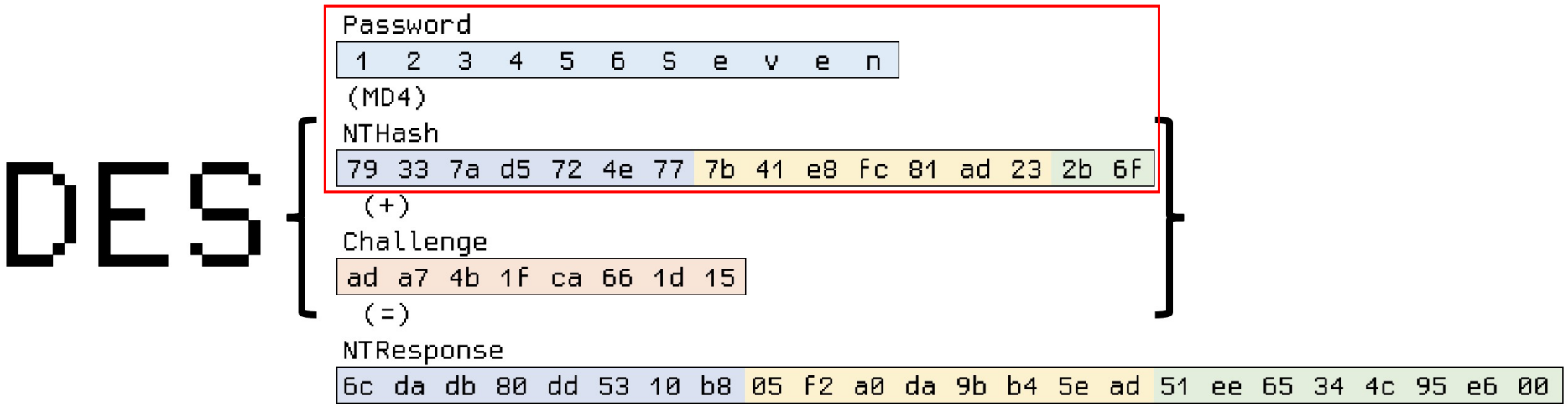
NTResponse Generation



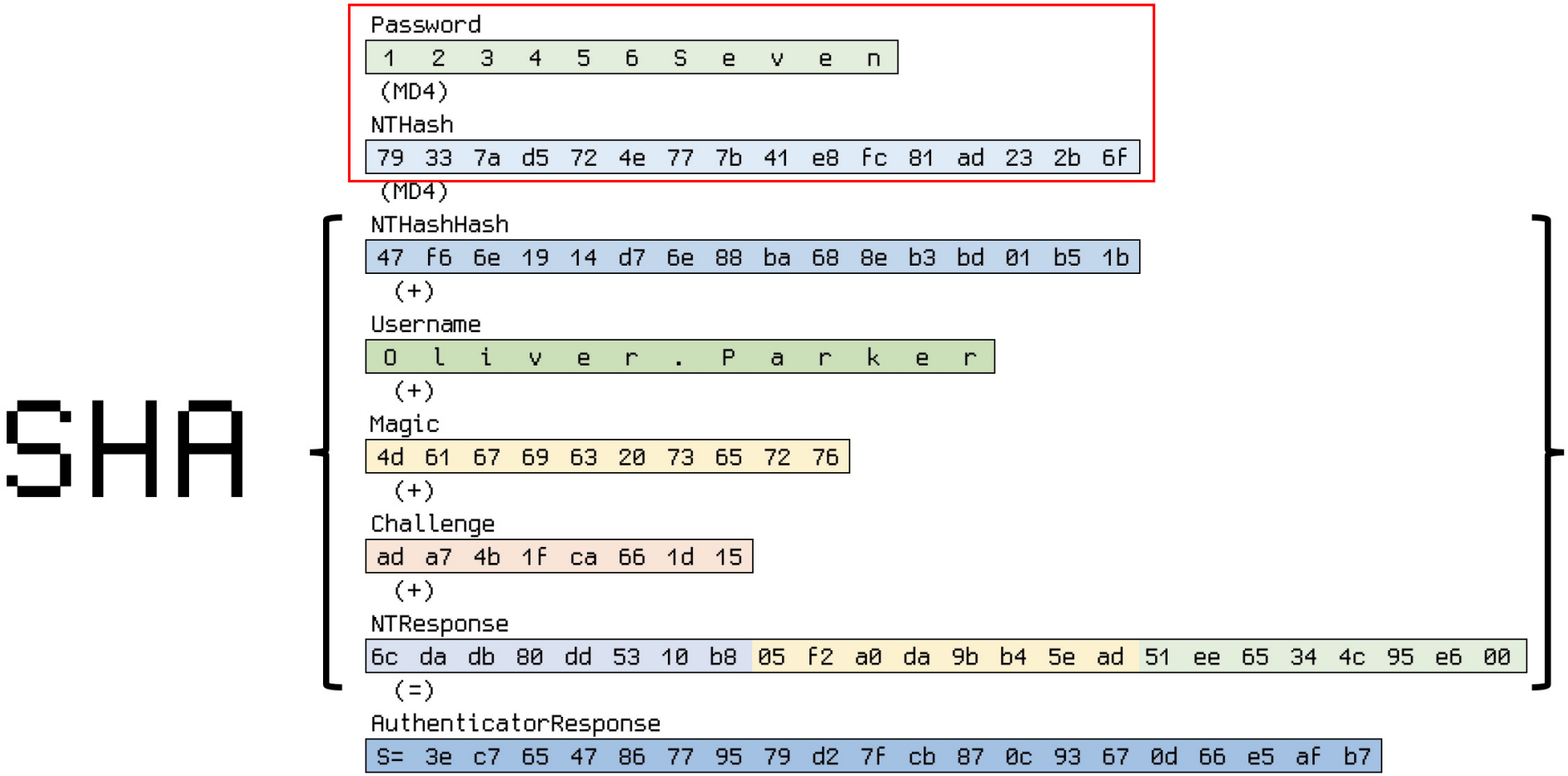
AuthenticatiorResponse Generation



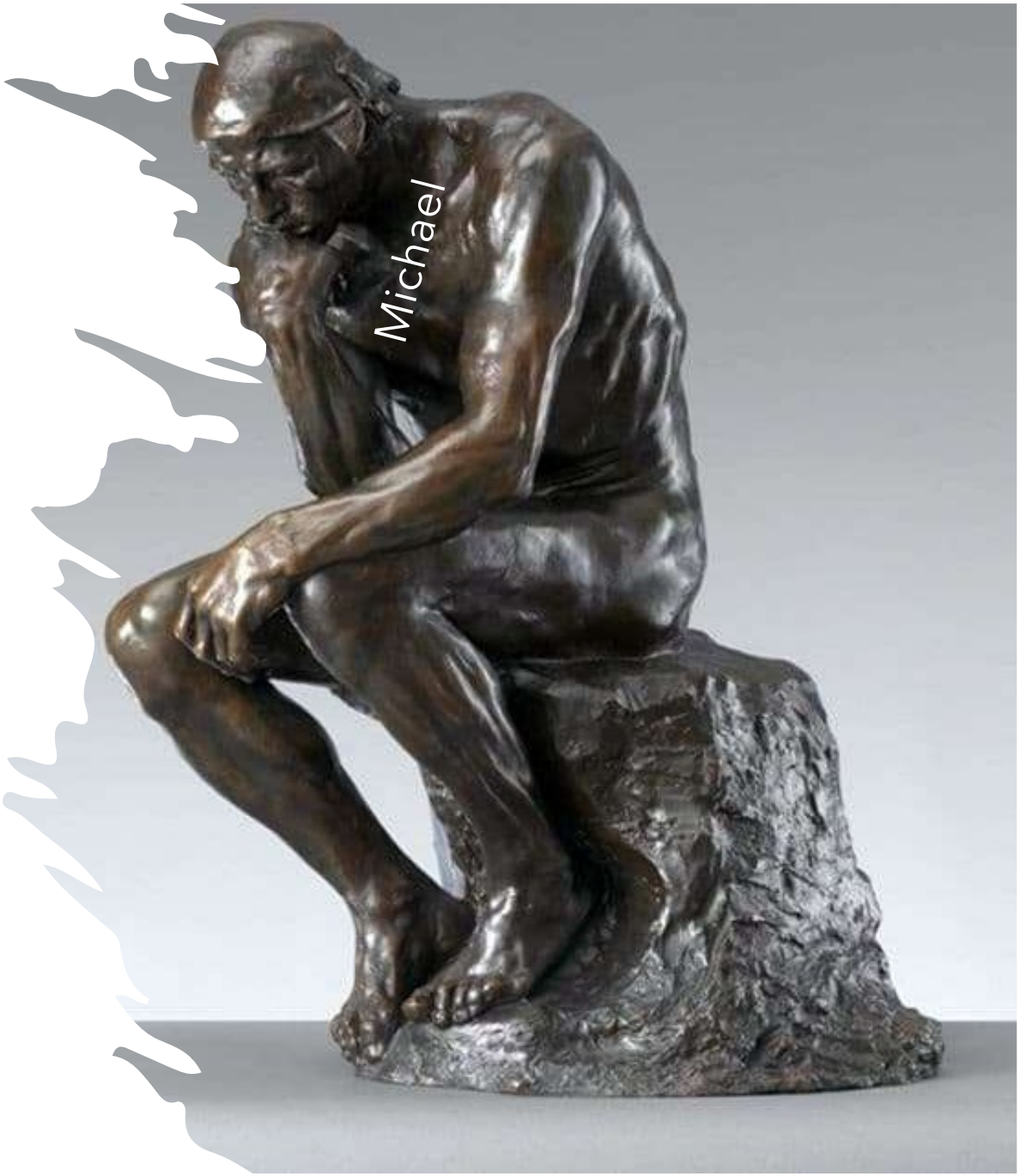
NTResponse Generation



AuthenticatiorResponse Generation



MSCHAPv2
hmmmmmm…




NT Hash


Pass the Hash

hostapd & wpa_supplicant support it

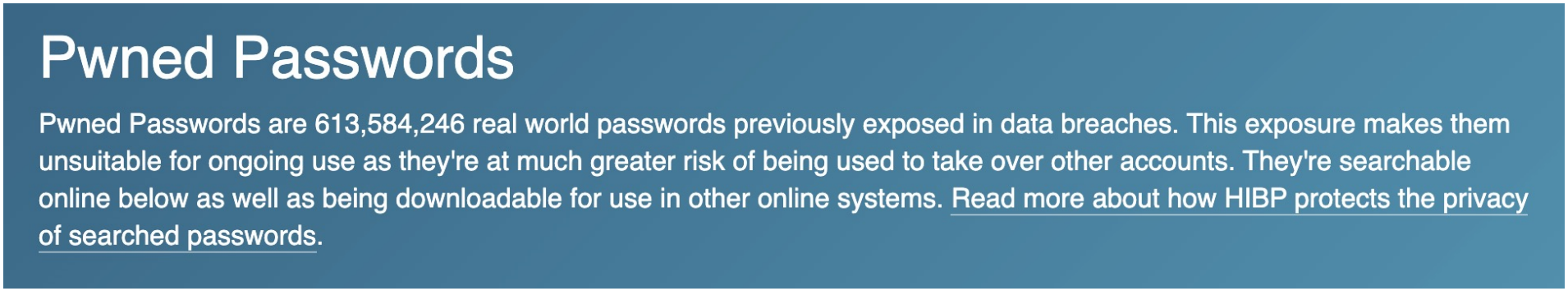
```
network={
        ssid="example"
        scan_ssid=1
        key_mgmt=WPA-EAP
        eap=PEAP
        identity="Oliver.Parker"
        password="hash:79337ad5724e777b41e8fc81ad232b6f"
        ca_cert="/etc/cert/ca.pem"
        phase1="peaplabel=0"
        phase2="auth=MSCHAPV2"
}
```

```
# Phase 1
*       PEAP

# Phase 2 (tunnelled within EAP-PEAP or EAP-TTLS) users
"Oliver.Parker" MSCHAPV2 hash:79337ad5724e777b41e8fc81ad232b6f [2]
```

Hashlists instead of Wordlists

- Current MSCHAPv2 modes take long
- There are a lot of wasted NThashes if you only use cracked ones
- There are places you can get NT hashes
  - Have I been Pwned, Active Directory, etc



Hashcat Forums 2016

How to make use of the DES KPA mode

atom
Administrator

09-03-2016, 11:39 AM

Just wanted to make a quick writeup how to use the new DES

An interessting example, I thought, would be how to retrieve
the server to enforce some challenge or if you sniffed it from

Reversing MSCHAPv2 to NTLM

evilmog
Junior Member

10-01-2016, 03:46 AM (This post was last modified: 10-02-2016, 03:40

So as we all know mode 14000 generic DES can be used fo
promised. This demo used $99 format which is MSCHAPv2
here http://markgamache.blogspot.ca/2013/01/n...roken.h

My New Hashcat Modes

```
  5500 | NetNTLMv1 / NetNTLMv1+ESS
 27000 | NetNTLMv1 / NetNTLMv1+ESS (NT)
  5600 | NetNTLMv2
 27100 | NetNTLMv2 (NT)
```

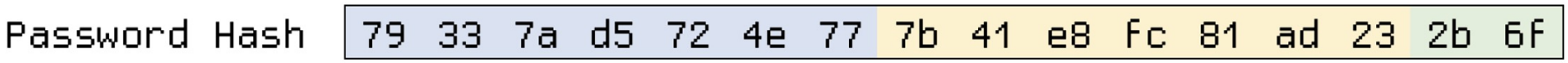
New Hashcat Modes Demo

Part of hashcat main branch as of 3 Aug 2021 (thanks atom)

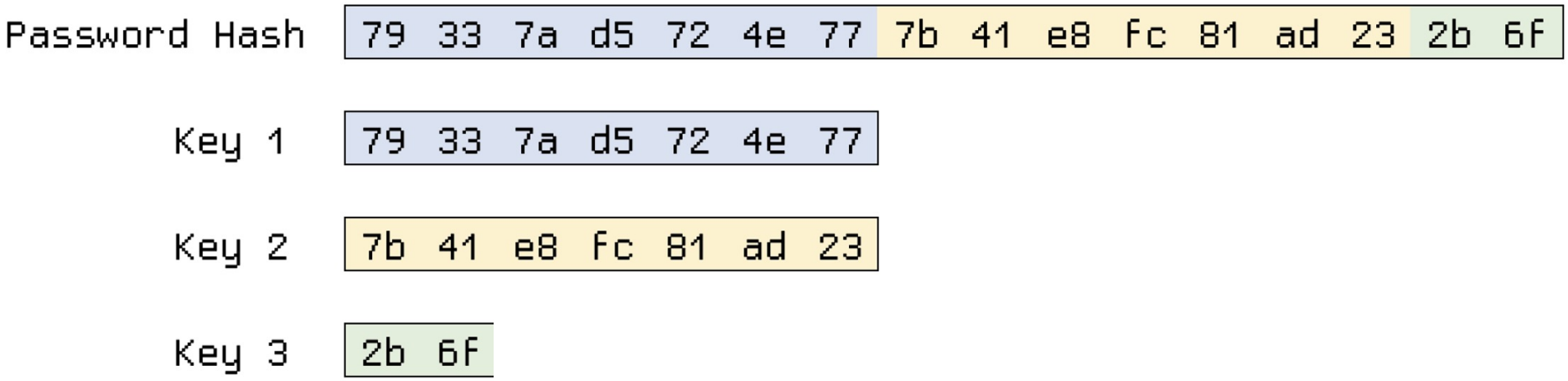
A new approach

Let's talk about the ~~arse~~ ass

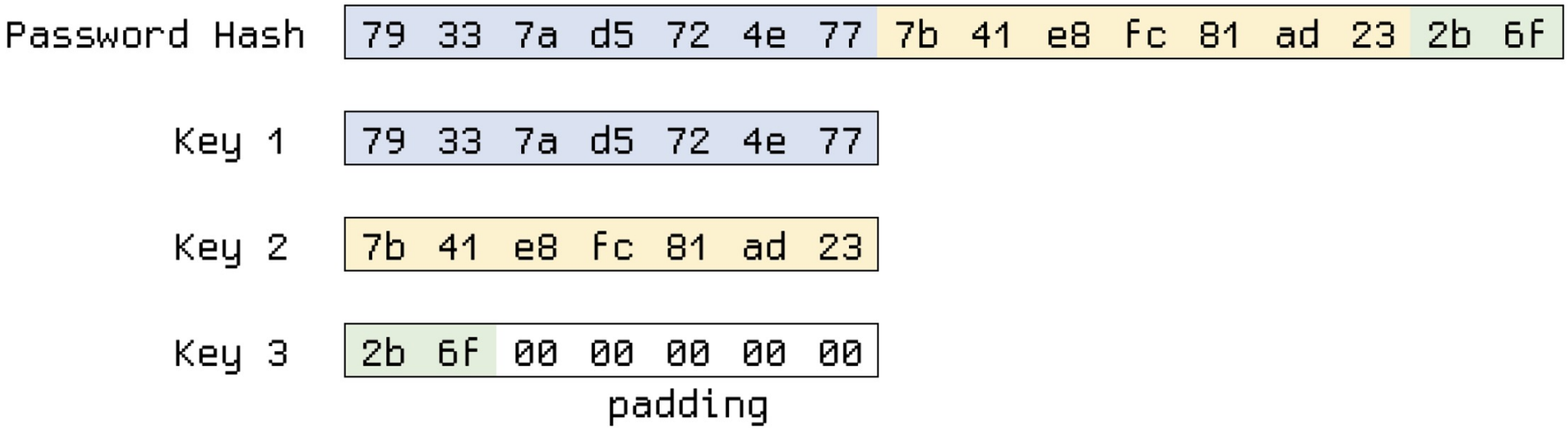
MSCHAPv2 NT Response DES Encryption



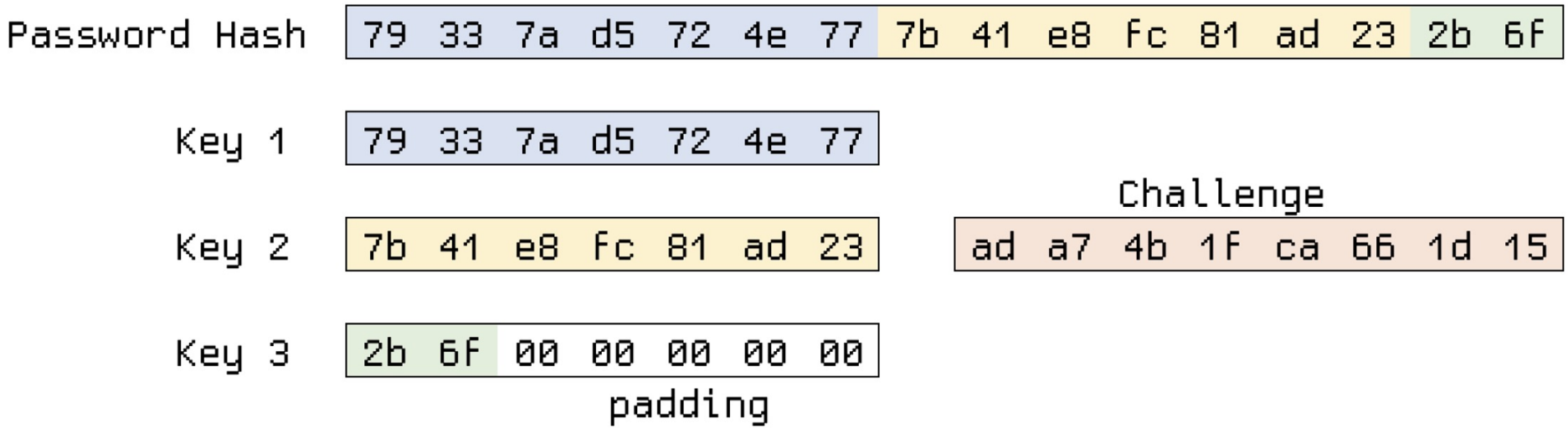
MSCHAPv2 NT Response DES Encryption

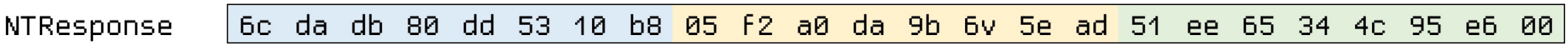


MSCHAPv2 NT Response DES Encryption

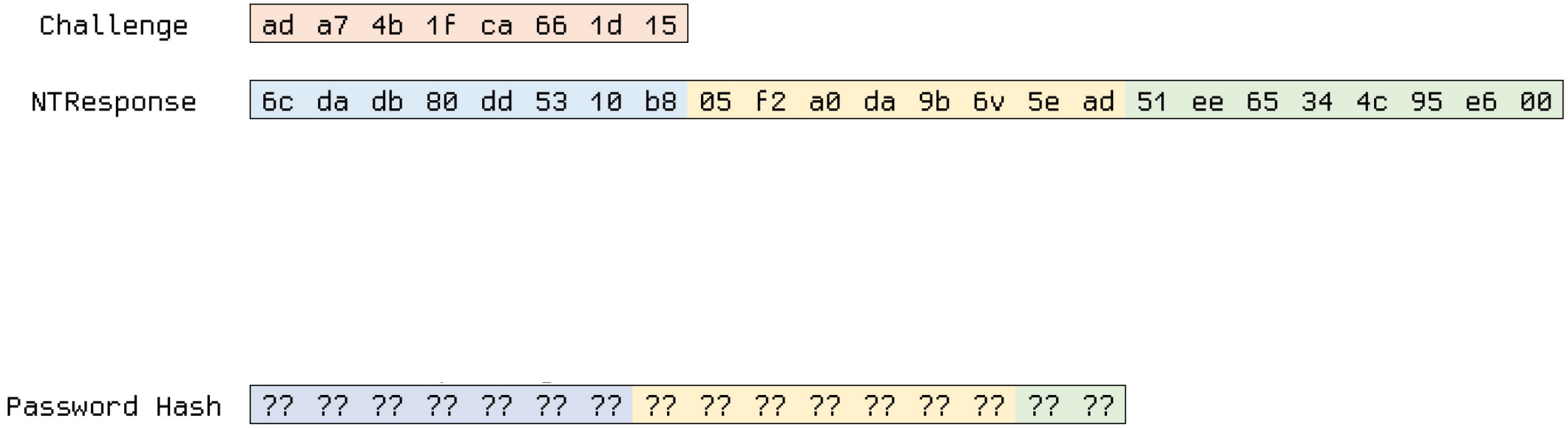


MSCHAPv2 NT Response DES Encryption

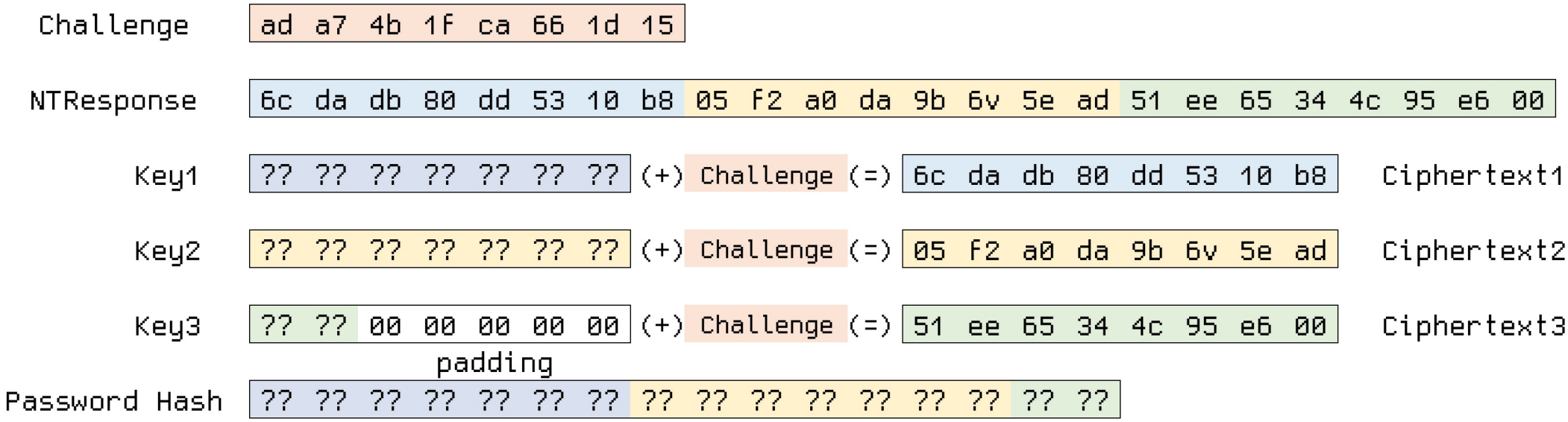




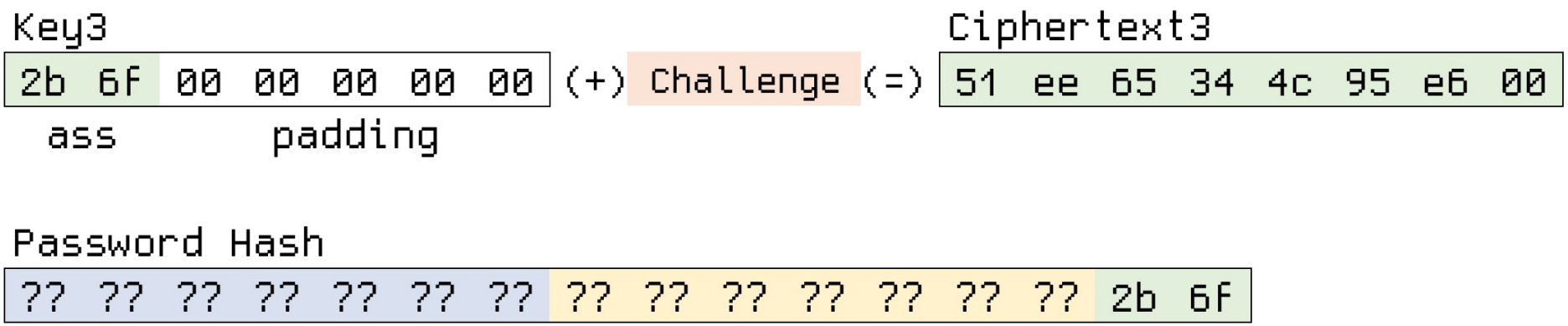
MSCHAPv2 Cryptanalysis



MSCHAPv2 Cryptanalysis



MSCHAPv2 Cryptanalysis - The Ass



Keyspace

0x0000 – 0xFFFF

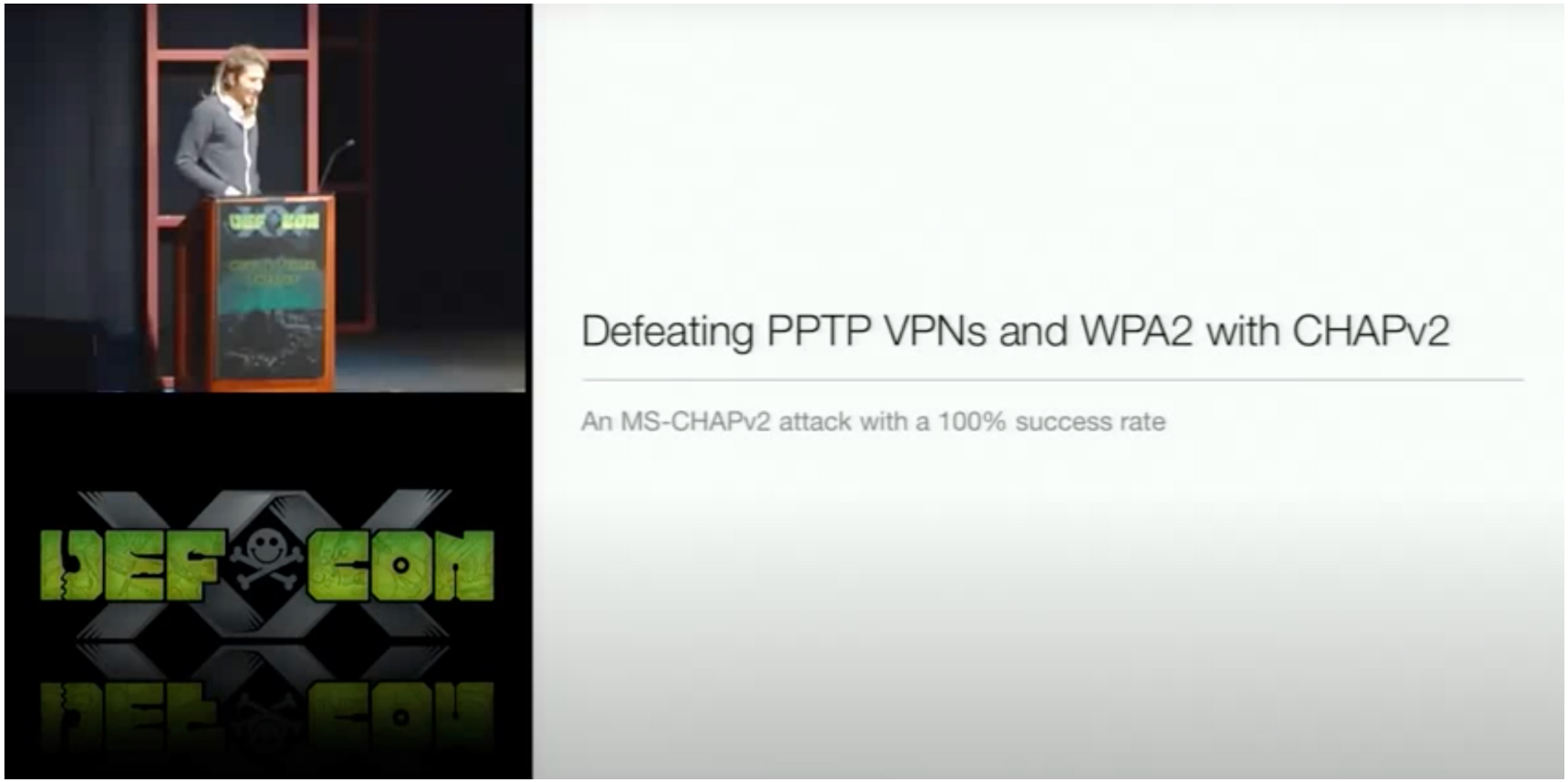
0 – 65535

Joshua Wright
DC11 2003

MS-CHAPv2 Weaknesses

- MS-CHAPv2 weaknesses apply to the LEAP exchange
  - No salt in stored NT hashes
    - Permits pre-computed dictionary attacks
  - Weak DES key selection for challenge/response
    - Permits recovery of 2 bytes of the NT hash
  - Username sent in clear-text
  - We can deduce authentication passwords

Moxie Marlinspike & David Hulton
DC20 2012



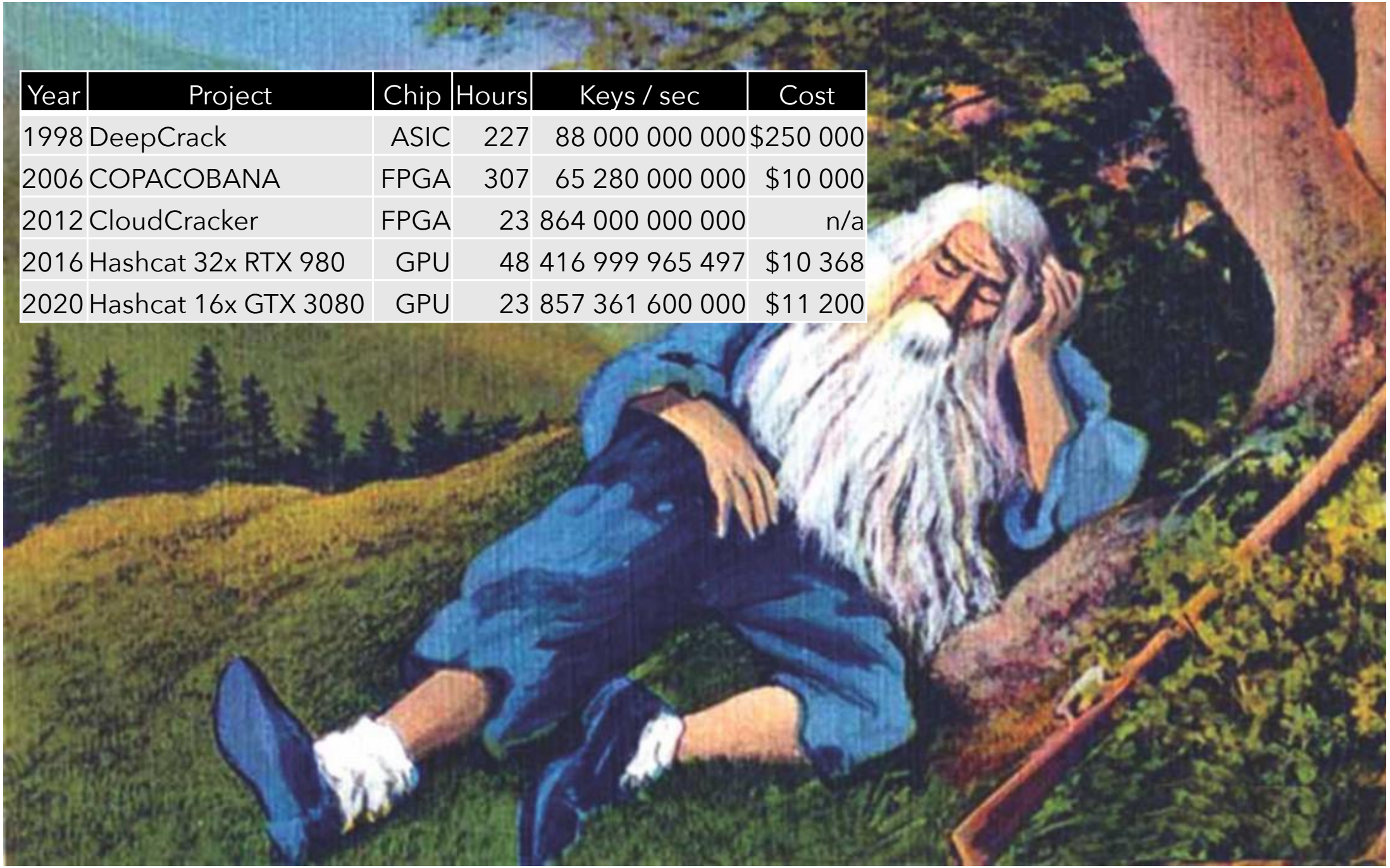
MSCHAPv2 Cryptanalysis
Single DES Round

Reduce two DES rounds to one - Encrypt once, compare twice

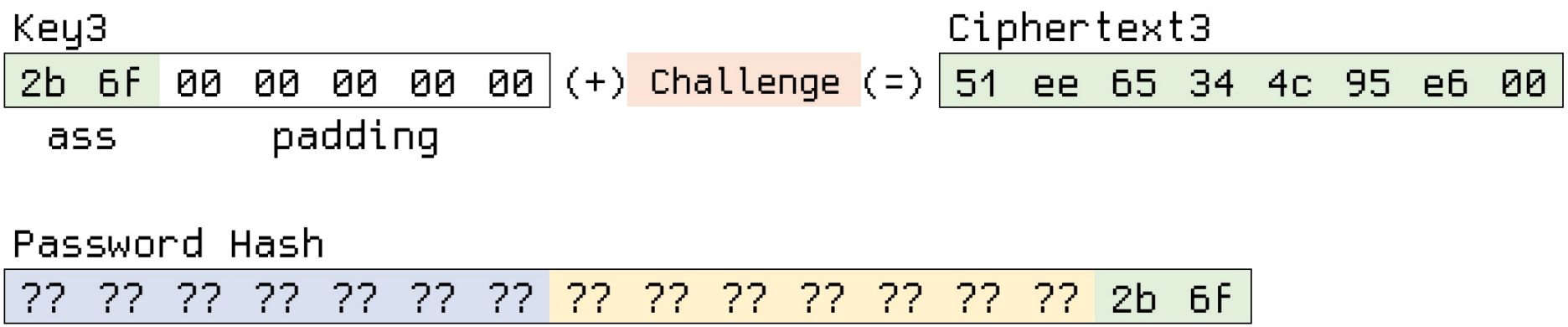
2^56 is 7 bytes aka 72 057 594 037 927 935

```
For i in 0 to 2^56
  result = DEScrypt(cleartext=challenge, key=i)
  if result == ciphertext1: key1 = i
  if result == ciphertext2: key2 = i
```

Year	Project	Chip	Hours	Keys / sec	Cost
1998	DeepCrack	ASIC	227	88 000 000 000	$250 000
2006	COPACOBANA	FPGA	307	65 280 000 000	$10 000
2012	CloudCracker	FPGA	23	864 000 000 000	n/a
2016	Hashcat 32x RTX 980	GPU	48	416 999 965 497	$10 368
2020	Hashcat 16x GTX 3080	GPU	23	857 361 600 000	$11 200



MSCHAPv2 doesn't protect its ass




```
grep 2b6f$ NTLM-hashlist.txt
```

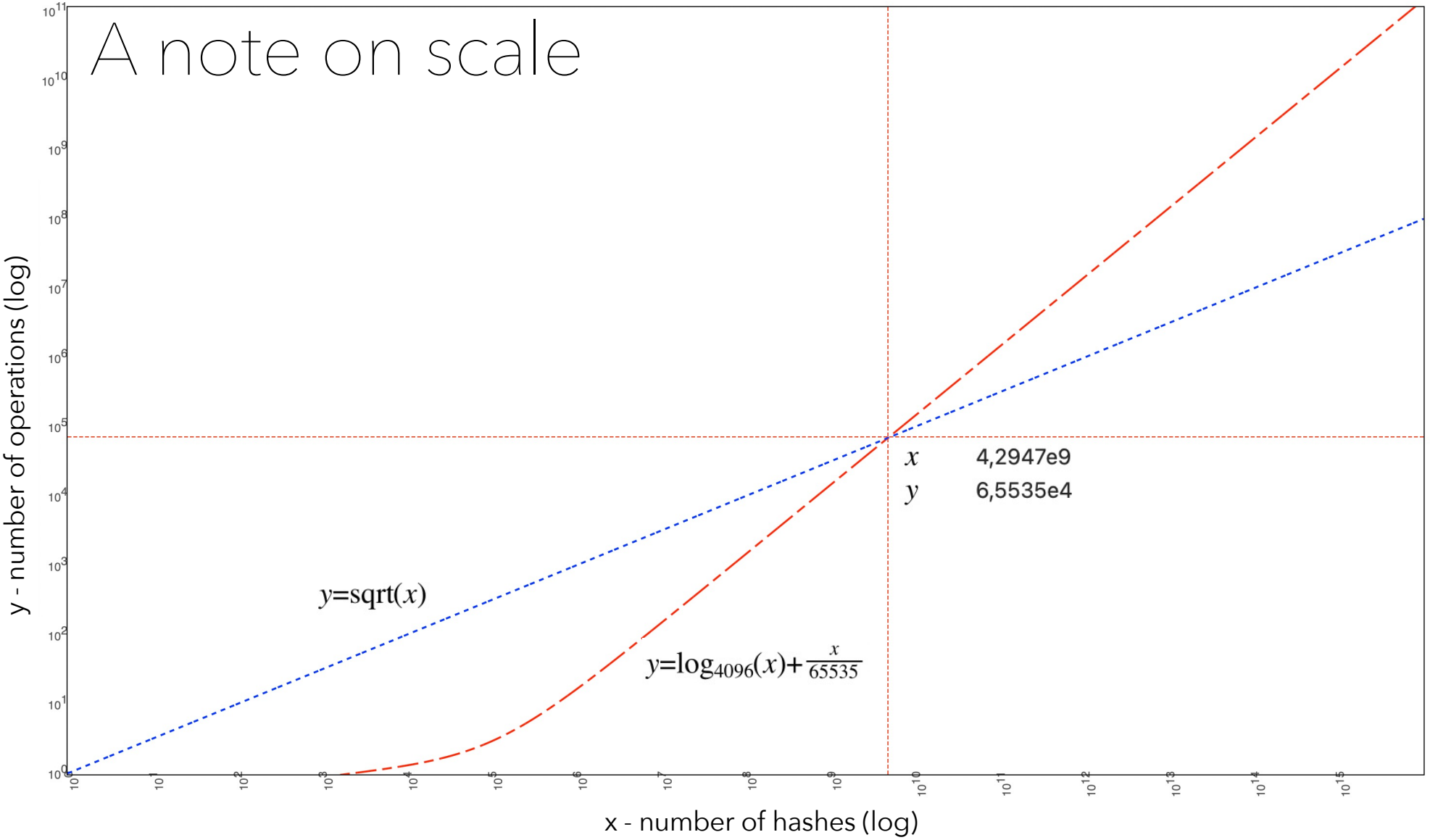
Initial (worst) Performance

hash	tool	small	HIBP
hash1	hashcat	8.778s (2250.6 kH/s)	2:58.84 (5662.4 kH/s)
	assless	0.860s	46.393s
hash2	hashcat	9.627s (1985.2 kH/s)	1:04.39 (5241.2 kH/s)
	assless	0.696s	41.152s


Bravely bold Sir Robin
Rode forth from Camelot


The Dark Path of Perf Optimisation
threading
rust!
indexes!
databases!
file tricks
two-byte lookups
ripgrep

A note on scale



Current (best) Performance

hash	small	rockyou	HIBP
hash1	19ms	19ms	17ms
hash2	11ms	13ms	12ms
hash3	11ms	11ms	63ms

Average: 20ms
Median: 13ms

Assless Demo

https://github.com/sensepost/assless-chaps/

Have I Been Pwned HashList Problems

123456 (23.2m)	ashley (432,276)	liverpool (280,723)	blink182 (285,706)	superman (333,139)
123456789 (7.7m)	michael (425,291)	chelsea (216,677)	50cent (191,153	naruto (242,749)
qwerty (3.8m)	daniel (368,227)	arsenal (179,095)	eminem (167,983	tigger (237,290_
password (3.6m)	jessica (324,125)	manutd (59,440)	metallica (140,841)	pokemon (226,947)
1111111 (3.1m)	charlie (308,939)	everton (46,619)	slipknot (140,833)	batman (203,116)

https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security

Hashcat Generated Hash Lists

Wordlist:

```
password
company_name
```

Rules:

- Add Numbers
- Add Dates
- Change Case

Results:

```
Password1
Password2
Password2021
AcmeCorp1
AcmeCorp2
AcmeCorp2021
```

Hashlist Generation Demo

https://github.com/sensepost/assless-chaps/

Wrap Up – Crackers Paradise

As I iterate candidates in the keyspace of DES
I take a look at my battery life
And realise there's not much left
Cause I've been cracking this hash so long
That even my momma thinks that my life is gone
But I ain't never cracked a hash that didn't deserve it
Hashcat says 25 years, will I ever reach 24?
The way things are going I don't know

Tell me why are we, so blind to see,
that a better way to crack,
is in front of you and me

Why are we doing this?

To recover an NT hash quickly

But why?

1. To pass the hash to NTLMv1 endpoints
2. To connect to Wi-Fi or PPTP VPNs
3. To host rogue Wi-Fi access points

In Summary

1. MSCHAPv2 used the NTHash not the clear text password
2. You can use full NT hash lists, including the uncracked
3. New hashcat modes 27000 & 27100 for NTLMv1 & NTLMv2
4. MSCHAPv2 exposes its ass (easy brute of last two bytes)
5. These can reduce the hashlist to crack against
6. Index'ed DB lookups cost less than DES brute-forces
    1. At less than 17 billion hashes (average case)

Greetz & Shouts

- Orange Cyberdefense Hackathon Team
  - Darryn, Aurelien, Charly
- Atom and Chick3nman for hashcat module writing help
- Joshua Wright for asleap
- Moxie & David for cloudcrack
- Chick3nman for hash shucking
- https://github.com/sensepost/assless-chaps/