

Crypto 101

A “no crazy maths” guide to breaking crypto

Benjamin Kearns – Technical Team Leader

Event – OWASP Day 2015

Date – 27th February 2015

Company Overview

Company

- Lateral Security (IT) Services Limited
- Founded in April 2008 by Nick von Dadelszen and Ratu Mason (Both Directors)
- Auckland, Wellington Melbourne: ~20 highly specialised security consultants

Services

- Security testing (design & architecture, penetration testing, configuration, code reviews, security devices & controls, mobile apps)
- Security advisory (Lifecycle compliance & audit – ISO, PCI-DSS, NZISM, policy process development, threat modeling and risk assessment)
- Regular ongoing technical testing and assurance programs



Me

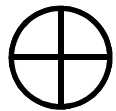


Overview

- Introduction
- XOR
- Stream ciphers
- Block cipher modes
 - Electronic Codebook (ECB)
 - Cipher Block Chaining (CBC)
- HMAC



XOR (Exclusive Or)



0 XOR 0 = 0

1 XOR 0 = 1

0 XOR 1 = 1

1 XOR 1 = 0

0100	1011	(P)
\oplus 1100	1110	(K)
<hr/>		
1000	0101	(C)

1000	0101	(C)
\oplus 1100	1110	(K)
<hr/>		
0100	1011	(P)

XOR – Example

Plain text: Secret String

Key: a

Secret String XOR aaaaaaaaaaaaaa

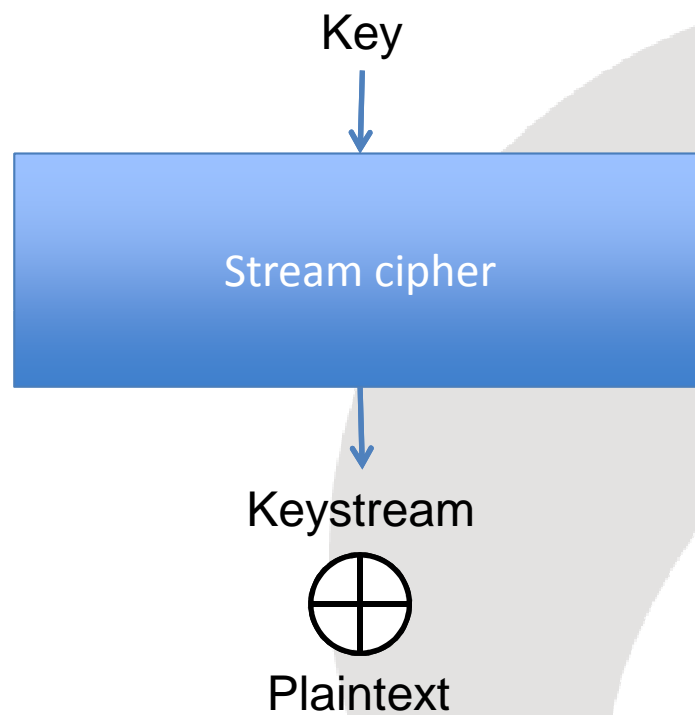
0101 0011 0110 0101 0110 0011 ..

0110 0001 0110 0001 0110 0001 ..

0011 0010 0000 0100 0000 0010 ..

32 04 02 13 04 15 41 32 15 13 08 0f 06

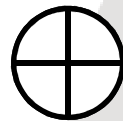
Stream ciphers



Stream Ciphers

“Secret Session Key” → Stream Cipher → 492485C29AF129B...

492485C29AF129B...



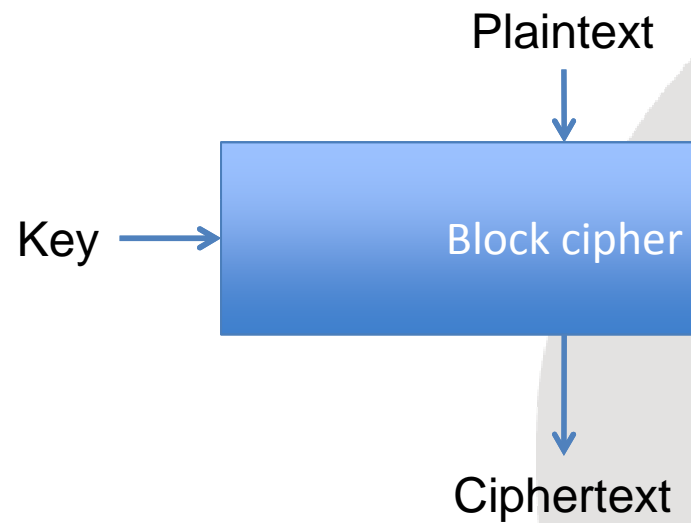
uid=4;cart_items=[502,388,590,4]



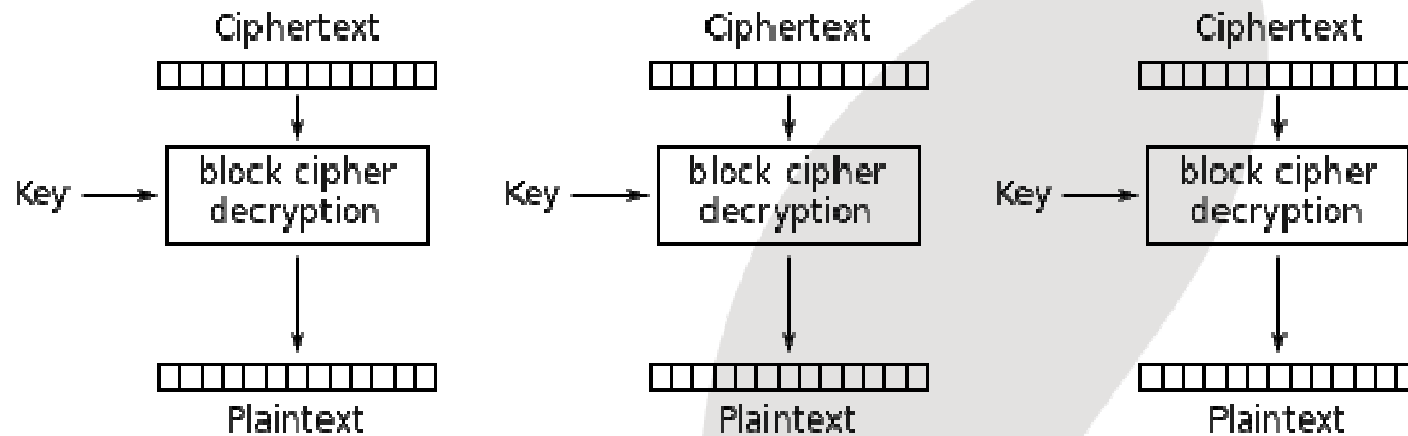
But you're safe, right?



Block ciphers



Electronic Codebook (ECB)



Electronic Codebook (ECB) mode decryption

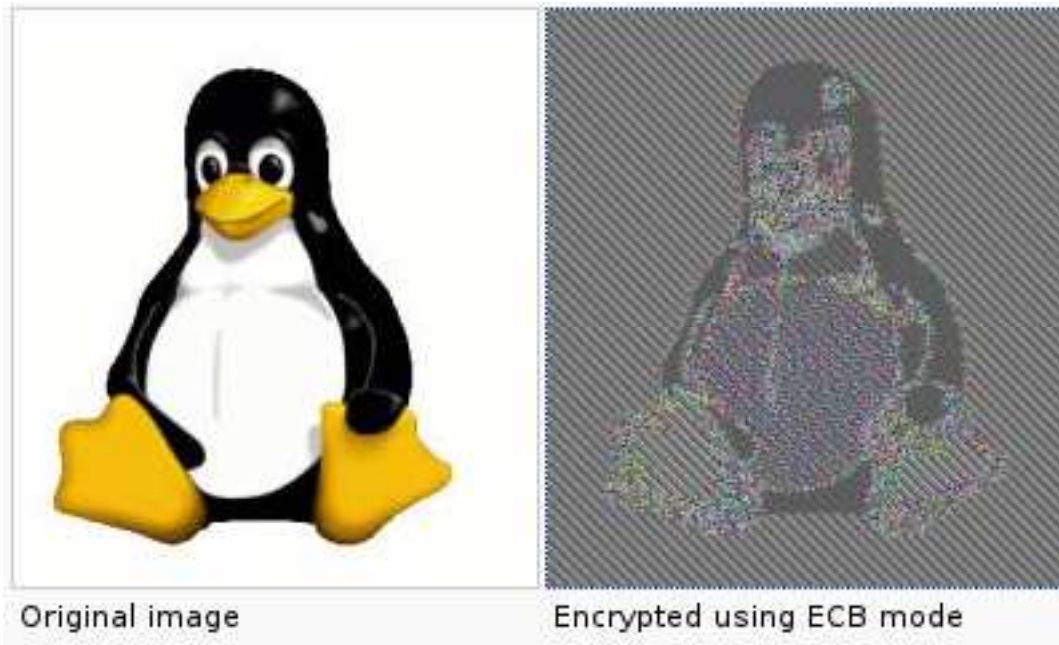
ECB example

AAAAAAAABBBBBBBBBAAAAAAAAA

AAAAAAAA | BBBBBBBB | AAAAAAAAA

a49e184729a65b18 | 38f9c215972c28e3 | a49e184729a65b18

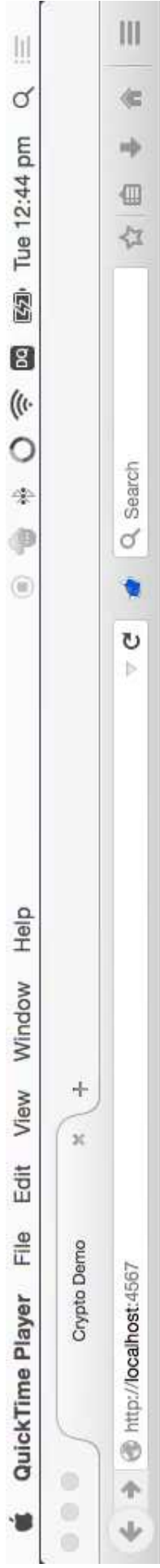
ECB Example



Exploiting ECB

SITE_ID=1;ADMIN=02;USER=492;LOGIN_TIMESTAMP=1375861043;

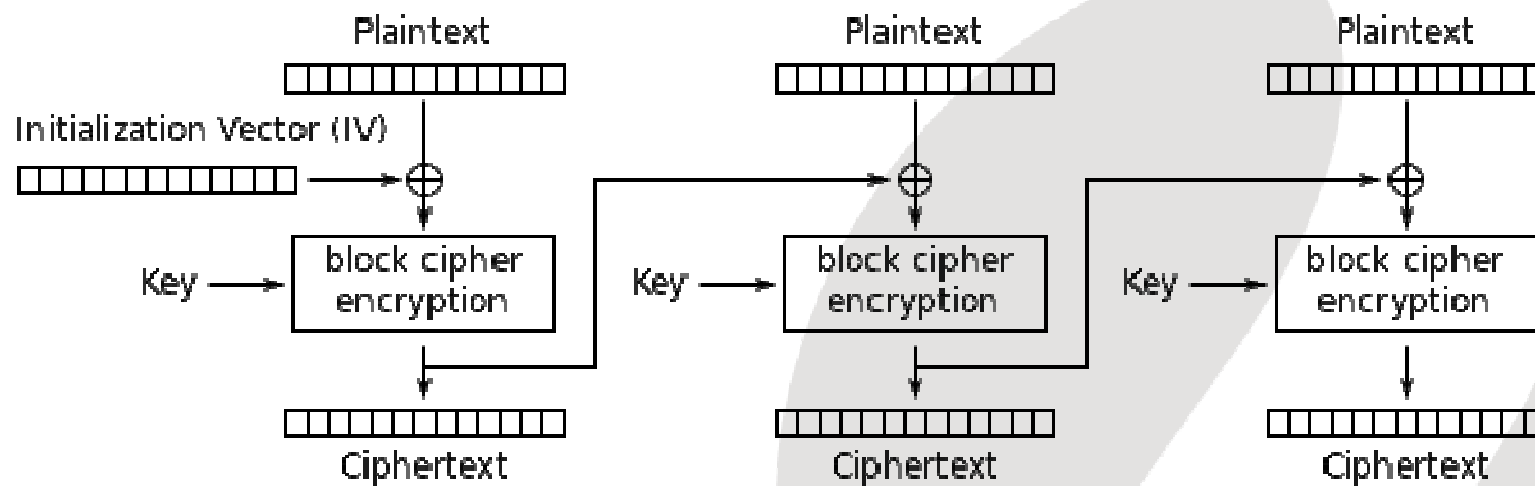
```
function process_session_cookie() {  
SITE_ID= 0358f292249283bc  
session_cookie = decrypt_cookie(COOKIES['Session'])  
1;ADMIN= 49f28b20a3c3051d  
variables = session_cookie.split(';')  
02;USER=4 58382d298f9526f5  
02;LOGIN 48a84d294c128646  
foreach(session_variable in variables) {  
key_value_array = session_variable.split('=')  
_TIMESTAMP= 193b48cff29ac493  
session[key_value_array.first] = key_value_array.second;  
MP=13758 104d210c20a04882  
61043; 294859ac4980a5dd  
}  
  
//...  
  
if(session['ADMIN'] != 0) {  
SESSION=0358f292249283bc49f28b20a3c3051d58382d298f9526f548a84d29  
// unlock awesome admin powers  
4c128646193b48cff29ac493104d210c20a04882294859ac4980a5dd  
}
```



But you're safe, right?

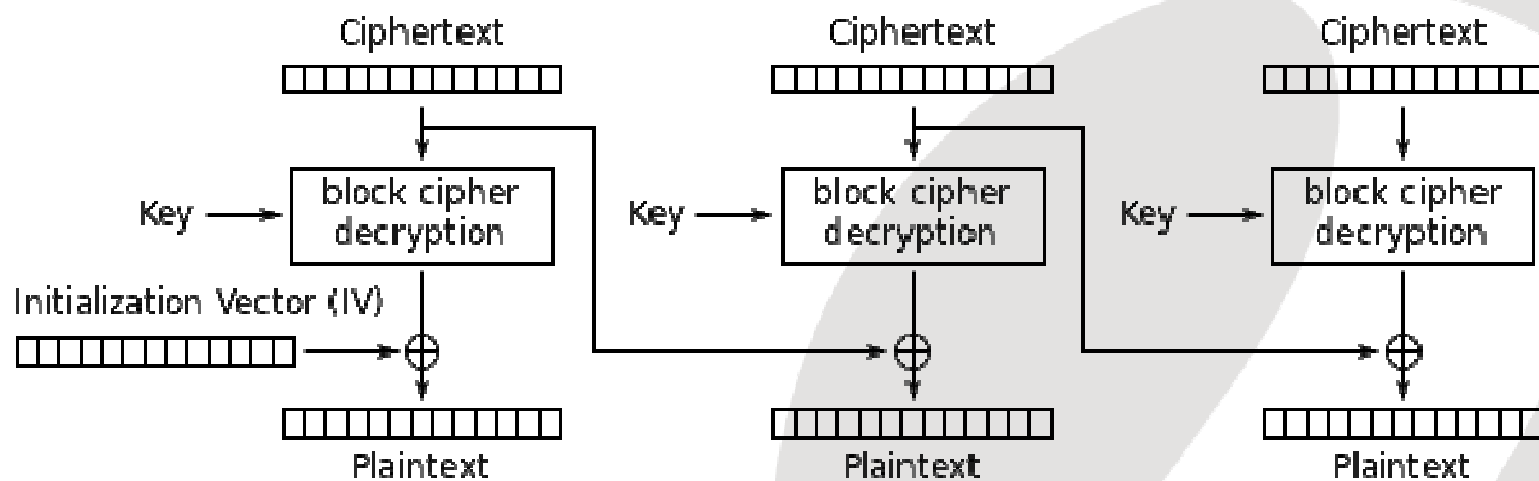
```
Cipher cipher = Cipher.getInstance("AES");  
Cipher.init(...)
```

CBC



Cipher Block Chaining (CBC) mode encryption

CBC



Cipher Block Chaining (CBC) mode decryption



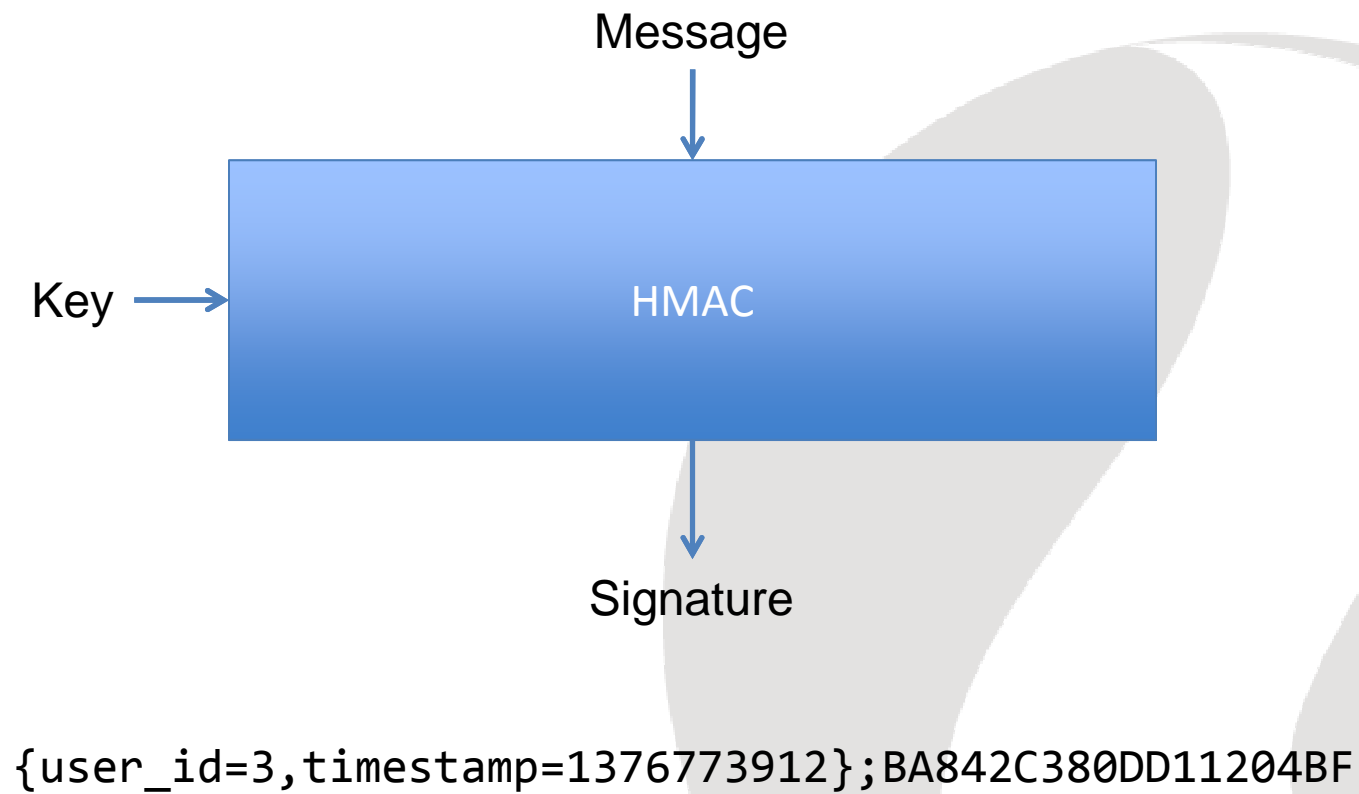
But you're safe, right?



CISCO TM

CVE-2005-0039

HMAC





User:

Password:



But you're safe, right?



B1347247976a6c5fba55f3f81faba1c8b6777e55
6015824405f06b4dbcea65b433535f7ad747ce36



0a38e9a40ca5d66d7002a6ade0ed0f8b71058c82
0163f66cf65d91521ab55255ff708b9909b13800
8a7f13d68fec575def1dc3ff7200cd72b0658963
15e0bed2

Cracking crypto



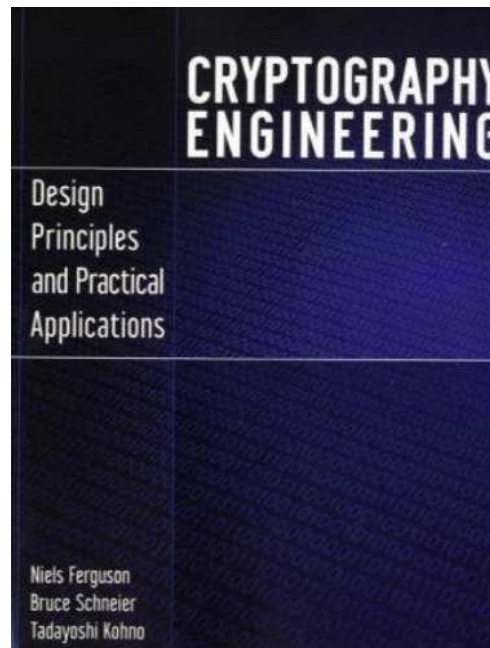
Top Secret



Computers are hard



More crypto fun



<http://www.matasano.com/articles/crypto-challenges/>

Questions and Contacts



Presentation Download
[www.lateralsecurity.com/
presentations](http://www.lateralsecurity.com/presentations)

Lateral Security (IT) Services Limited

Wellington

38-42 Waring Taylor Street (level 7, Petherick Tower)
PO Box 8093, Wellington 6143, New Zealand
Phone: +64 4 4999 756
Email: sas@lateralsecurity.com

Auckland

187 Queen Street (level 8, Landmark House)
PO Box 7706, Auckland, New Zealand
Phone: +64 9 3770 700
Email: sas@lateralsecurity.com

Melbourne

200 Queen Street (level 13)
Melbourne, VIC 3000, Australia
Phone: +61 1300 554745
Email: sas@lateralsecurity.com