Cryptanalysis – a Never-Ending Story

Anne Canteaut

Inria, Paris, France

University of Bergen - October 16, 2019

Big data = big security breaches

Marriott Mega-Breach: Victim Count Drops to 383 Million

Hotel Giant Warns 5.3 Million Unencrypted Passport Numbers Also Stolen

Mathew J. Schwartz (euroinfosec) · January 7, 2019

Twitter Facebook LinkedIn Credit Eligible Get Permission

JW Marriott Venice Resort & Spa in Italy (Photo: Marriott International)

Marriott International says its recently discovered mega-breach isn't quite as bad as first advertised, in terms of the total number of victims. But it also warns that hackers stole 5.25 million unencrypted passport numbers that its hotels were storing as well as 8.6 million encrypted payment cards

https://www.databreachtoday.com/marriott-mega-breach-victim-count-drops-to-383-million-a-11916

Sensitive data

Healthcare under Attack: What Happens to Stolen Medical Records?

30 czerwca 2016

According to reports from news portal Deep Dot Web, 689,621 patient records are being sold by a hacker operating in TheRealDeal, a deep web marketplace known for peddling stolen data, codes and zero-day software exploits. The hacker told the news site that he used an exploit in how the organizations utilize remote desktop protocol (RDP), adding that it is a specific security flaw with precise conditions needed for it to be triggered.

The hacker, who goes by the handle "thedarkoverlord," is offering a purportedly one-off copy of the stolen data. The data has been broken into databases, with prices ranging from 151 to 643 bitcoins (BTC), amounting to around US$96,000 to $411,000

Powiązane art

- Unsecure Pagers in Vancouver Expose Se Patient Data: What Th Means for Enterprise
- Recognizing Enterpri Mission-Critical Asset
- License Plates, Photo Passwords and More Two Separate Breach
- Ransomware Hits Co Offices, Knocks The Channel Offline
- Android Malware Can SimBad Adware and Operation Sheep Rep Installed 250 Million

Najnowsze art

https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/healthcare-under-attack-stolen-medical-records

Attacks

In most attacks, cryptography is bypassed.

"I am not aware of any major world-class security system employing cryptography in which the hackers penetrated the system by actually going through the cryptanalysis." [Adi Shamir 2002]

Attacks

https:

//afroginthefjord.com/2014/07/12/why-the-french-are-so-arrogant-and-why-norwegians-arent/

However...

- biases in RC4 [AlFardam et al. 13]
- Logjam [Adrian et al. 15]: weak Diffie-Helman
- Sloth [Bhargavan, Leurent 16]: collisions in MD5

FLAME spy malware

BBC Sign in News Sport Reel Worklife Travel Future

NEWS

Home Video World UK Business Tech Science Stories Entertainment & Arts

Technology

Flame: Attackers 'sought confidential Iran data'

By Dave Lee
Technology reporter, BBC News

4 June 2012 Share

The attackers behind the massive Flame malware were seeking to obtain technical drawings from Iran, researchers have said.

Analysis by Kaspersky Lab suggested that the huge majority of targets were within the country.

The malware network, which was revealed last week, has since stopped operating.

The characteristics of Flame have seen it compared to past Stuxnet and Duqu

The malware appears as a Windows Update security patch, with a valid certificate.

The fraudulent signature has been forged with a chosen-prefix collision attack against MD5 [Stevens 07]

Attacks against MIFARE

COMPUTERWORLDUK
THE VOICE OF BUSINESS TECHNOLOGY

Features Technology IT Business Careers Tut

Resources

Home 〉 News 〉 IT Vendors 〉 Questions raised about Oyster card security

Questions raised about Oyster card security

Its RFID chip is cracked by researchers

Network World and Computerworld UK staff
March 7, 2008

re **Smartcards with encrypted RFID chips, including London's Oyster fare card, might not be as secure as previously thought.**

Can we trust cryptographers?

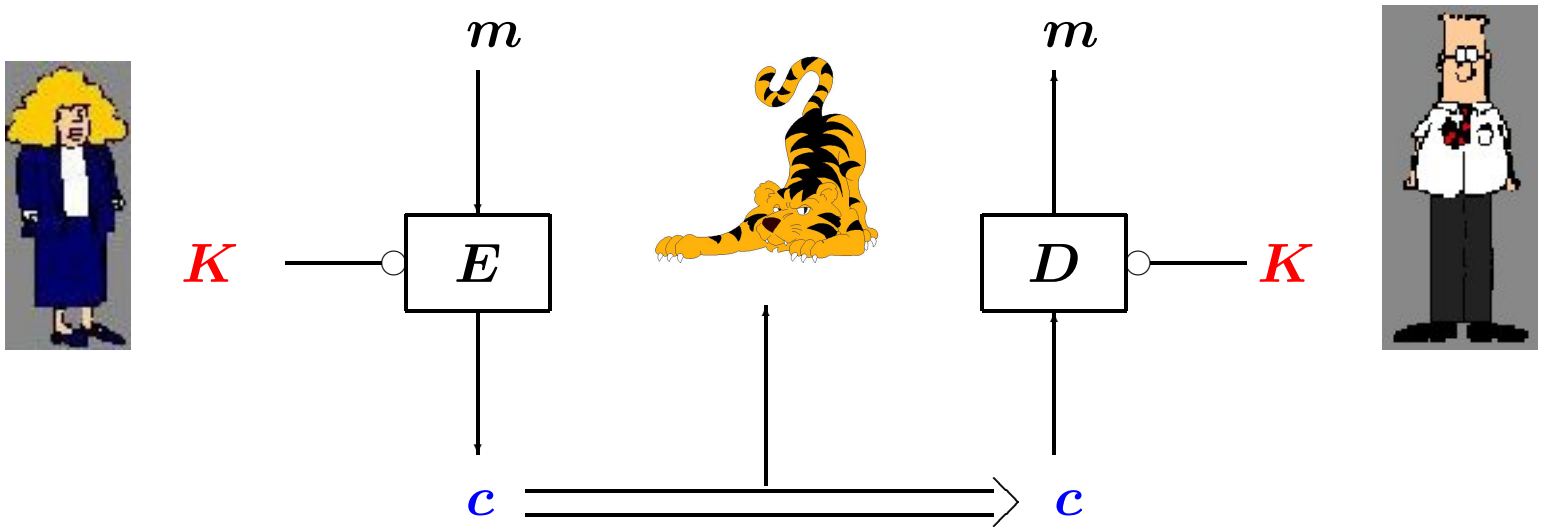
Kerckhoffs' principles (1883)

The system must not require secrecy and can be stolen by the enemy without causing trouble.

The Administration must absolutely renounce secret methods, and must establish in principle that it will only accept a process that can be taught publicly in our military schools, that our students will be free to to communicate to whomever they want.

A cipher

K is a secret key.



Perfect secrecy [Shannon 49]

"For all ciphertexts, the *a posteriori* probabilities for the various messages are equal to the *a priori* probabilities independently of the values of these."

Intercepting the message has given the cryptanalyst no information.

For any pair (m, c),

$$\mathbf{Pr}[M = m | C = c] = \mathbf{Pr}[M = m].$$

Equivalently,

$$\mathbf{Pr}[C = c | M = m] = \mathbf{Pr}[C = c].$$

There is at least one key transforming any plaintext m into any of the ciphertexts c.

$\longrightarrow$ nb of keys $\geq$ nb of possible plaintexts.

Vernam cipher [Vernam 1926]

plaintext	u	n	b	r	e	a	k	a	b	l	e
	20	13	1	17	4	0	10	0	1	11	4
secret key	n	w	l	r	b	b	m	q	b	h	c
	13	22	11	17	1	1	12	16	1	7	2
ciphertext	7	9	12	8	5	1	22	16	2	18	6
	h	j	m	i	f	b	w	q	c	s	g

The Signal Corps tested the secrecy of communications handled by the system and tried it out between New-York and Washington. This trial proved that the system could be successfully used to send messages secretly.

Vernam cipher [Vernam 1926]

plaintext	u n b r e a k a b l e
secret key	n w l r b b m q b h c
ciphertext	h j m i f b w q c s g

plaintext	i n f o r m a t i o n
secret key	z w h u o p w x u e t
ciphertext	h j m i f b w q c s g

The plaintext and the ciphertext are statistically independent.

$$\mathbf{Pr}[C = c|M = m] = \mathbf{Pr}[C = c].$$

Practical secrecy

measure of the amount of work required to break the system

Breaking:

- recover the plaintext from the ciphertext;
- recover the key from the knowledge of some plaintext-ciphertext pairs.

Amount of work:

- time;
- memory;
- data.

Paranoia?

Cryptanalysis of the full Spritz [Banik, Isobe 16]:

"We need approximatively 2^{1247} assignments to recover the internal state."

Paranoia?

Cryptanalysis of the full Spritz [Banik, Isobe 16]:

"We need approximatively 2^{1247} assignments to recover the internal state."

$$2^{1247} \simeq 10^{375} \gg (\#\text{ atoms in the universe })^4$$

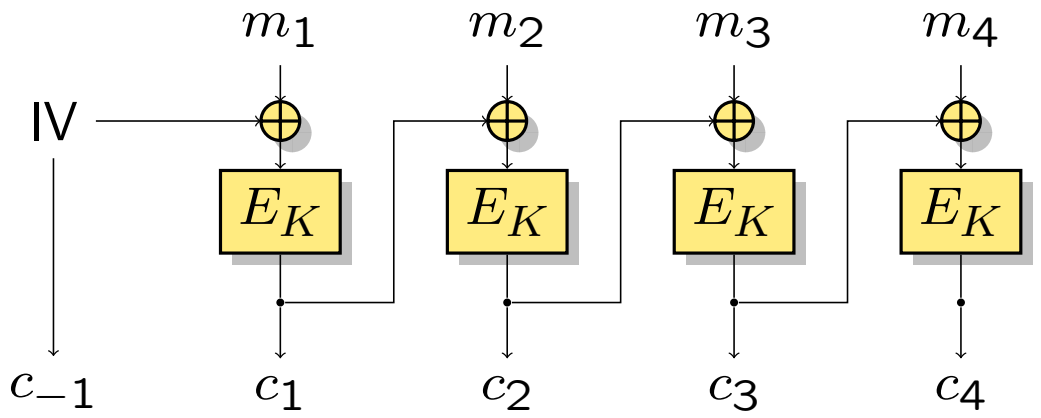
What is cryptanalysis about?

A good primitive must behave as a function chosen at random from the set of all functions with the same characteristics.

Symmetric Encryption Schemes

For encrypting messages of an arbitrary length:

- use a transformation operating on n-bit blocks (block cipher)
- chain the blocks with a mode of operation (CBC, CTR...)



Typical block size:

$$n \in \{128, 64\}$$

Ideal block cipher

A block cipher operating on n-bit messages with a k-bit key

$$\Longleftrightarrow$$

2^k permutations of the set of n-bit messages, randomly selected among the $2^n!$ possible ones.

Ideal block cipher

A block cipher operating on n-bit messages with a k-bit key

$$\Longleftrightarrow$$

2^k permutations of the set of n-bit messages, randomly selected among the $2^n!$ possible ones.

Requirement. These permutations P cannot be distinguished from a randomly selected permutation from the knowledge of some pairs $(x, P(x))$.

Ideal behavior

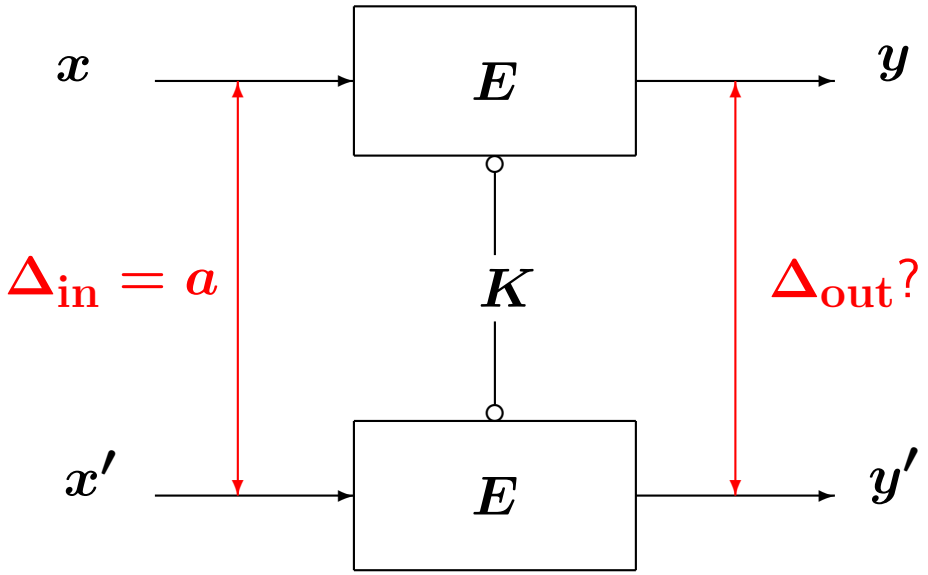
A block cipher operating on n-bit messages with a k-bit key

$$\Longleftrightarrow$$

2^k permutations of the set of n-bit messages, randomly selected among the $2^n!$ possible ones.

No attack better than brute-force: There is no attack having a complexity significantly less than the cost of 2^k evaluations of the cipher.

Differential cryptanalysis [Biham-Shamir 90]



For a random permutation π of n-bit messages, for any nonzero a and b,

$$\Pr_X[\pi(X + a) - \pi(X) = b] = \frac{1}{2^n - 1}$$

Broken?

A good primitive must behave as a function chosen at random from the set of all functions with the same characteristics.

Cryptanalysis of the full Spritz [Banik, Isobe 16]:

"We need approximatively 2^{1247} assignments to recover the internal state."

Specifications of Spritz [Rivest, Schulz 15]:

Spritz generates a pseudo-random sequence from a secret state, chosen out of 2^{1730} possibilities.

The internal state can be recovered with 2^{1247} trials $\rightarrow$ much better than brute-force.

Practical relevance?

But this is not relevant in our applications...

Finding collisions is not an issue in key-exchange protocols.

Sloth attack against TLS [Bhargavan, Leurent 16]:

exploits collisions in MD5!

But these attacks are not practical...

Attacks reveal unexpected weaknesses.

But these attacks are not practical...

Attacks reveal unexpected weaknesses.

Attacks always get better; they never get worse.

If cryptographers say that an algorithm is broken, don't use it!

Is there any difference between

- **AES** (NIST FIPS 197)
- **Crypto-1** (MIFARE Classic encryption)
- **Dual-EC-DRBG** (NIST SP 800-90A)

AES has been standardized after an open competition (1997-2001)

The foundation of trust

Hash function competition (SHA-3)

Oct 2008	submission deadline
	$\longrightarrow$ 64 candidates received by the NIST
Dec 2008	51 candidates in the 1st round
Feb 2009	1st SHA-3 conference

Let's start the struggle!

Abacus	Neil Sholer	in round 1	2nd-preimage	
ARIRANG	Jongin Lim	in round 1		
AURORA	Masahiro Fujita	in round 1	2nd preimage	
Blender	Colin Bradbury	in round 1	collision, preimage	near-collision
Boole	Greg Rose	in round 1	collision	
Cheetah	Dmitry Khovratovich	in round 1		length-extension
CHI	Phillip Hawkes	in round 1		
CRUNCH	Jacques Patarin	in round 1		length-extension
DCH	David A. Wilson	in round 1	collision	
Dynamic SHA	Xu Zijie	in round 1	collision	length-extension

http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo

Hash function competition (SHA-3)

Oct 2008	submission deadline
	$\longrightarrow$ 64 candidates received by the NIST
Dec 2008	51 candidates in the 1st round
Feb 2009	1st SHA-3 conference
July 2009	14 candidates in the 2nd round
Aug 2010	2nd SHA-3 conference
Dec 2010	5 finalists
Mar 2012	3rd SHA-3 conference
Oct 2012	winner announced (Keccak)

Prize for the best cryptanalysis

Third cryptanalysis prize

30 September 2009

We announce the third prize for the most interesting cryptanalysis of KECCAK. The results must be publicly available on an URL that is sent to keccak *-at-* noekeon *-dot-* org **before December 5, 2009** at 23:59 GMT+1 (i.e., before Sinterklaas or Saint Nicolas).

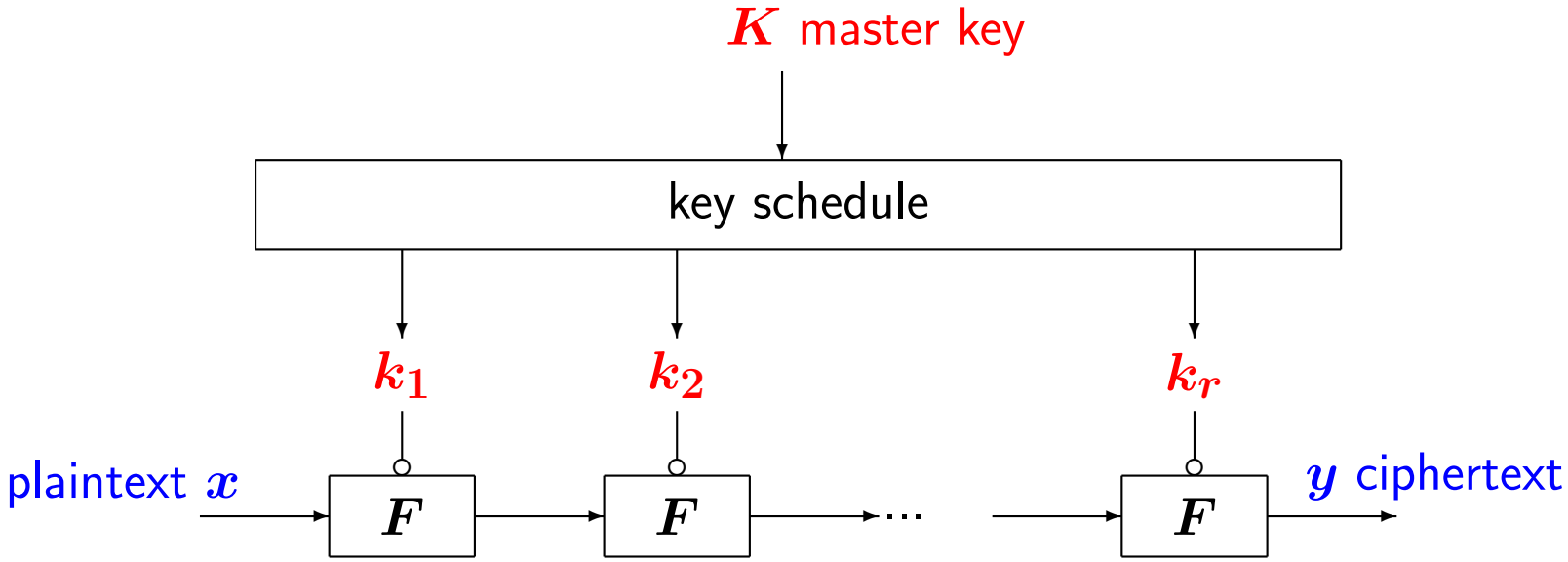
The third prize consists of beer, like the first one. This time we offer Lambic beers that according to myth can only be brewed in the surroundings of Brussels thanks to wild yeast and mysterious bacteria that would not occur anywhere else. Anyway, the prize is a case with 24 (the new number of rounds in KECCAK-*f*) bottles of Lambic-based beers from breweries such as Cantillon, Girardin, and 3 Fonteinen.

http://keccak.noekeon.org/third_party.html

Prize for the best cryptanalysis

[Boura, Canteaut 2011]: distinguisher on the inner permutation of Keccak with complexity 2^{1575} (instead of 2^{1600}).

Iterated block ciphers



where F is a keyed permutation of $\{0,1\}^n$.

How many rounds can we break?

AES-128 (10 rounds)[Daemen, Rijmen 98]:

5 rounds	2^{46}	Daemen, Rijmen 1998
5 rounds	2^{24}	Bar-On et al. 2018
6 rounds	2^{71}	Daemen, Rijmen 1998
6 rounds	2^{48}	Ferguson et al. 2000
7 rounds	$\simeq 2^{128}$	Gilbert, Minier 2000
7 rounds	2^{117}	Lu, Dunkelman, Keller, Kim 2008
7 rounds	2^{110}	Mala et al. 2010
7 rounds	2^{99}	Derbez, Fouque, Jean 2013

$\rightarrow$ a never-ending evaluation of the security margin is needed

"Stay critical!" [Daemen 11]

Cryptanalysis: foundation of trust

No public analysis, no trust

Examples:

- Crypto-1 (Mifare): proprietary design
- Dual-EC-DRBG: backdoor
- Simon, Speck [NSA 2015]: no design rationale
- Streebog, Kuznyechik [FSB 2015]: structure that cannot possibly be the outcome of a random generation process, contrary to the claims of the designers [Perrin 19]

New targets

New functionnalities

New threats

Forbes

SEP 4, 2015 | FORBES

Forbes: Quantum Computing: From Theory To Reality

Author: Jason Bloomberg

"The word quantum often portends New Age mumbo-jumbo, in spite of the fact that quantum mechanics underlies many of today's most important technologies, including lasers and the semiconductors found in every computer chip.

New implementation constraints

NIST Lightweight Competition

`https://csrc.nist.gov/Projects/lightweight-cryptography`

Feb 2019	submission deadline
	$\longrightarrow$ 57 candidates received by the NIST
Aug 2019	32 candidates in the 2nd round
Nov 2019	NIST lightweight workshop
Sept 2020?	finalists

2nd-round lightweight candidates

ACE
DryGASCON
ForkAE
Grain-128AEAD
KNOT
ORANGE
Pyjamask
Saturnin
SPIX
Subterranean 2.0
WAGE

ASCON
Elephant
GIFT-COFB
HyENA
LOTUS/LOCUS-AEAD
Oribatida
Romulus
SKINNY-AEAD
SpoC
SUNDAE-GIFT
Xoodyak

COMET
ESTATE
Gimli
ISAP
mixFeed
PHOTON-Beetle
SAEAES
SPARKLE
Spook
TinyJAMBU

Conclusion

Public analysis is the only reliable security argument