OTP and AES: A Historical Transition Between two Systems of Cryptography

Valdemar Thanner
Supervised by Mr. Bernhard Keller
Linguistic supervision by Ms. Margrit Oetiker

Kantonsschule Zug

06.03.2017

Overview

A Brief Overview of Cryptography

OTP

AES: The Advanced Encryption standard

- High Level Structure
- Rounds

A Historical Transition

- Conflicts Throughout History
- Cryptography in Our Society

Questions

A Brief Overview of Cryptography

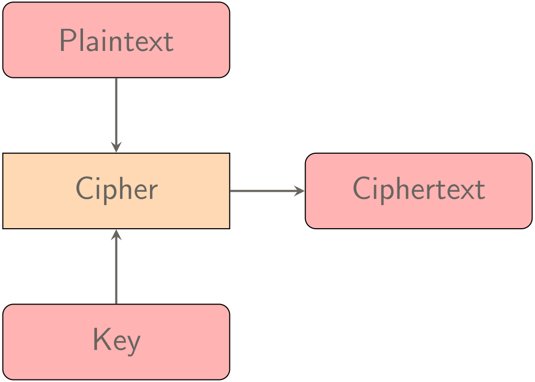
OTP

AES: The Advanced Encryption standard
- High Level Structure
- Rounds

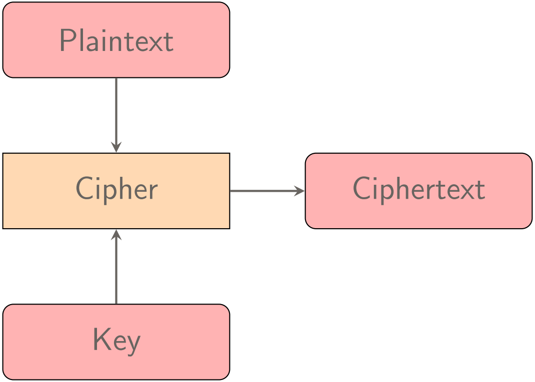
A Historical Transition
- Conflicts Throughout History
- Cryptography in Our Society

Questions

What is Cryptography?



What is Cryptography?



- "The art of writing or solving codes"
- The study of creating or breaking ciphers

A Brief Overview of Cryptography

OTP

AES: The Advanced Encryption standard
- High Level Structure
- Rounds

A Historical Transition
- Conflicts Throughout History
- Cryptography in Our Society

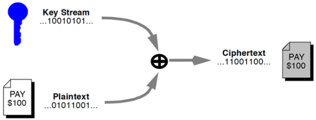
Questions

OTP: The One Time Pad

- Great historical impact
- Basis for or important part of many of today's modern algorithms
- The key must be disposed of securely after being used once
- Symmetrical cipher: Keeping of a shared secret

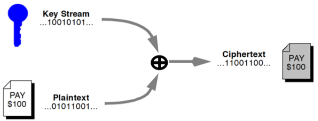
OTP: The Cipher

- Stream Cipher
- Key length $\geq$ Message length
- Based on modular addition
- Perfect (forward) secrecy



OTP: The Cipher

- Stream Cipher
- Key length $\geq$ Message length
- Based on modular addition
- Perfect (forward) secrecy



$$b + d = 1 + 3 = 4 = e$$
$$j + t = 9 + 19 = 28$$
$$(9 + 19) \mod 26 = 2 = c$$

OTP: The Cipher

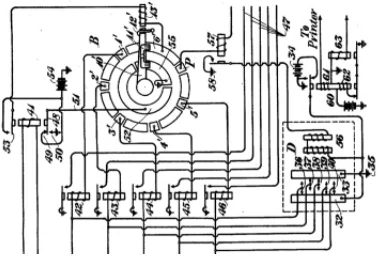
$$\begin{array}{cccccccccccc} c & r & y & p & t & o & g & r & a & p & h & y \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 17 & 24 & 15 & 19 & 14 & 6 & 17 & 0 & 15 & 7 & 24 \end{array}$$

$$\begin{array}{cccccccccccc} s & y & t & r & u & i & f & q & n & i & h & m \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 18 & 24 & 19 & 17 & 20 & 8 & 5 & 16 & 13 & 8 & 7 & 12 \end{array}$$

$$\begin{array}{cccccccc} 2+18 & 17+24 & 24+19 & 15+17 & 19+20 & 14+8 & 6+5 & 17+16 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 20 & 15 & 17 & 6 & 13 & 22 & 11 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ u & p & r & g & n & w & l & h \end{array}$$

OTP: A Precursor to Modern Computer-aided Cryptography

- Gilbert Vernam: Secret signaling system of 1919



OTP: A Precursor to Modern Computer-aided Cryptography

- Gilbert Vernam: Secret signaling system of 1919
- Looping perforated tape: known-plaintext vulnerability
- Bits: Binary digits

A Brief Overview of Cryptography

OTP

AES: The Advanced Encryption standard

High Level Structure

Rounds

A Historical Transition

Conflicts Throughout History

Cryptography in Our Society

Questions

A Brief Overview of Cryptography

OTP

AES: The Advanced Encryption standard
High Level Structure
Rounds

A Historical Transition
Conflicts Throughout History
Cryptography in Our Society

Questions

AES: Terminology

- Bit: Boolean value first conclusively described by Claude Shannon

$0 \vee 1$

AES: Terminology

- Bit: Boolean value first conclusively described by Claude Shannon

$0 \vee 1$

$(2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0)_b$
$(00000011)_b = 1 \cdot 2^1 + 1 \cdot 2^0 = 3$

- Byte: 8 Bits; can represent any number from 0-255

$(16 + 1)_h$ $1 - 9; A; B; C; D; E; F$
$(B4)_h = 16 \cdot 11 + 4 \cdot 1 = 180$

AES: Design Goals

- Confusion: Each bit of the ciphertext should depend on multiple bits of the key
- Diffusion: The "avalanche effect", small changes to the plaintext should strongly impact the ciphertext
- Two different implementations: Computationally or memory efficient

AES: The Advanced Encryption Standard

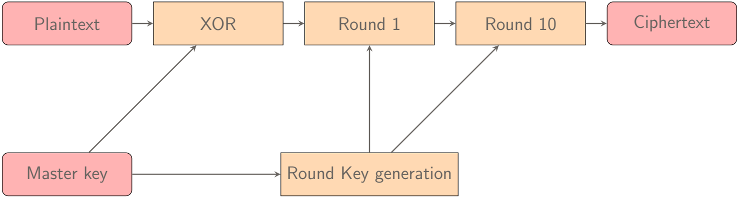
- Block Cipher
- The current N.I.S.T standard for SECRET and TOP-SECRET designated files
- Original name: Rijndael; was selected as the successor to DES.

AES: The Advanced Encryption Standard

- Block Cipher
- The current N.I.S.T standard for SECRET and TOP-SECRET designated files
- Original name: Rijndael; was selected as the successor to DES.

$$\begin{pmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \end{pmatrix}$$

AES: High-Level Structure



A Brief Overview of Cryptography

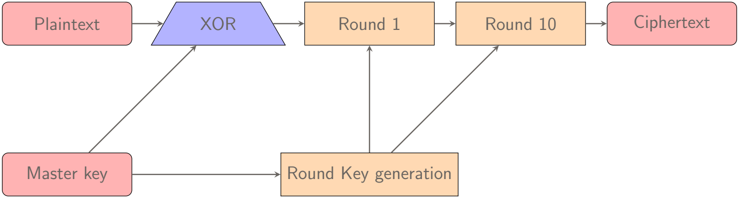
OTP

AES: The Advanced Encryption standard
- High Level Structure
- Rounds

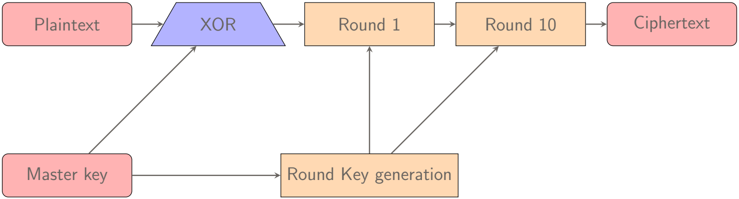
A Historical Transition
- Conflicts Throughout History
- Cryptography in Our Society

Questions

AES: Rounds

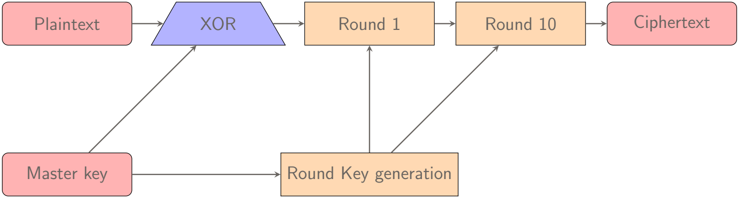

Plaintext
XOR
Round 1
Round 10
Ciphertext
Master key
Round Key generation

AES: Rounds



$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ \bigoplus & \bigoplus & \bigoplus & \bigoplus \\ 0 & 1 & 1 & 0 \\ = & = & = & = \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

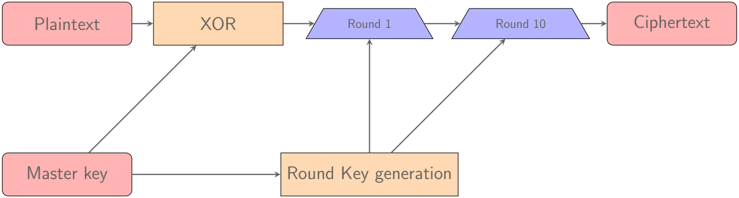
AES: Rounds



$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ \bigoplus & \bigoplus & \bigoplus & \bigoplus \\ 0 & 1 & 1 & 0 \\ = & = & = & = \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

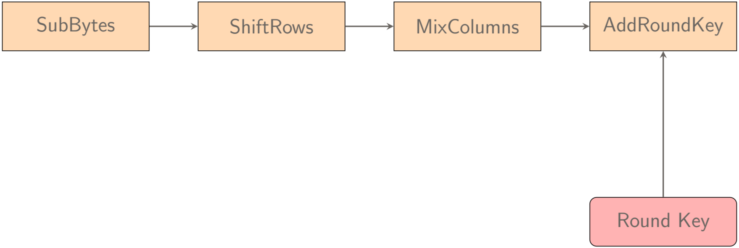
- bitwise logical operation; can be performed directly by the CPU
- addition mod 2
- can randomize biased input

AES: Rounds



Plaintext
XOR
Round 1
Round 10
Ciphertext
Master key
Round Key generation

AES: Rounds



AES: SubBytes

S-Box Values																
S(rs)	s															
r	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

AES: SubBytes

- Bytewise operation
- Sole source of Confusion; the only non-linear operation in AES (affine transformation)
- Key-independence is accepted in return for non-linearity; this eliminates one of DES' major weaknesses
- Utilization of the multiplicative inverse: if $a \cdot b = 1$ then $b = a^{-1}$
- Maximizes non-linearity, but negatively impacts diffusion: $0^{-1} = 0$ and $1^{-1} = 1$

AES: ShiftRows

$$\begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \xrightarrow{\text{ShiftRows}} \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,1} & a_{1,2} & a_{1,3} & a_{1,0} \\ a_{2,2} & a_{2,3} & a_{2,0} & a_{2,1} \\ a_{3,3} & a_{3,0} & a_{3,1} & a_{3,2} \end{pmatrix}$$

AES: ShiftRows

$$\begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \xrightarrow{\text{ShiftRows}} \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,1} & a_{1,2} & a_{1,3} & a_{1,0} \\ a_{2,2} & a_{2,3} & a_{2,0} & a_{2,1} \\ a_{3,3} & a_{3,0} & a_{3,1} & a_{3,2} \end{pmatrix}$$

- One of the two primary sources of diffusion
- One small change to the plaintext should result in a large change to the ciphertext
- Bytes are placed into the state in column order, but shifted across rows

AES: MixColumns

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix}$$

AES: MixColumns

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix}$$

$$s_0 = 02a_0 + 03a_1 + 01a_2 + 01a_3$$
$$\mathrm{s}_1 = 01a_0 + 02a_1 + 03a_2 + 01a_3$$
$$\mathrm{s}_2 = 01a_0 + 01a_1 + 02a_2 + 03a_3$$
$$\mathrm{s}_3 = 03a_0 + 01a_1 + 01a_2 + 02a_3$$

AES: MixColumns

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix}$$

$$\begin{aligned} s_0 &= 02a_0 + 03a_1 + 01a_2 + 01a_3 \\ s_1 &= 01a_0 + 02a_1 + 03a_2 + 01a_3 \\ s_2 &= 01a_0 + 01a_1 + 02a_2 + 03a_3 \\ s_3 &= 03a_0 + 01a_1 + 01a_2 + 02a_3 \end{aligned}$$

- Each new byte is dependent on an entire column of four old bytes
- Second source of diffusion

AES: AddRoundKey

- Identical to the initialing XOR
- XORs the round key with the state

$$\begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \bigoplus \begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{pmatrix}$$

A Brief Overview of Cryptography

OTP

AES: The Advanced Encryption standard
- High Level Structure
- Rounds

A Historical Transition
- Conflicts Throughout History
- Cryptography in Our Society

Questions

A Brief Overview of Cryptography

OTP

AES: The Advanced Encryption standard
- High Level Structure
- Rounds

A Historical Transition
- Conflicts Throughout History
- Cryptography in Our Society

Questions

The Crypto War: Past and Present

The Crypto War: Past and Present

- WWII: British Special Operations Executive

The Crypto War: Past and Present

- WWII: British Special Operations Executive
- Value of information: Rising exponentially alongside globalization

The Crypto War: Past and Present

- WWII: British Special Operations Executive
- Value of information: Rising exponentially alongside globalization
- Covert operations and proxy wars

The Crypto War: Past and Present

- WWII: British Special Operations Executive
- Value of information: Rising exponentially alongside globalization
- Covert operations and proxy wars

Motivator for more Powerful Computing

Motivator for more Powerful Computing

- Cryptologists vs. Cryptanalysts

Motivator for more Powerful Computing

- Cryptologists vs. Cryptanalysts
- Speed and Efficiency: RAM (Rapid Analytic Machines)

Motivator for more Powerful Computing

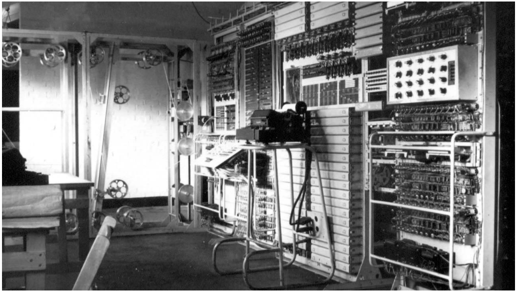
- Cryptologists vs. Cryptanalysts
- Speed and Efficiency: RAM (Rapid Analytic Machines)
- Each different problem required a specialized RAM

Motivator for more Powerful Computing

- Cryptologists vs. Cryptanalysts
- Speed and Efficiency: RAM (Rapid Analytic Machines)
- Each different problem required a specialized RAM
- Alan Turing's Thesis: Build a computer not restricted to one specific problem

Motivator for more Powerful Computing

- Cryptologists vs. Cryptanalysts
- Speed and Efficiency: RAM (Rapid Analytic Machines)
- Each different problem required a specialized RAM
- Alan Turing's Thesis: Build a computer not restricted to one specific problem
- Colossus: The world's first programmable computer

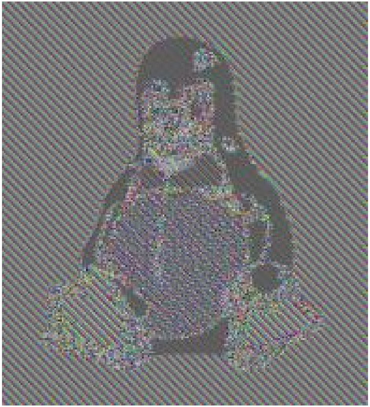


Today's Issues

- Mode of operation: ECB

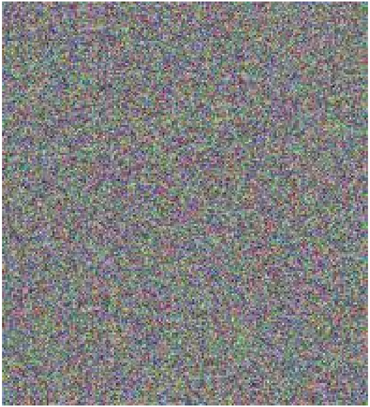
Today's Issues

- Mode of operation: ECB



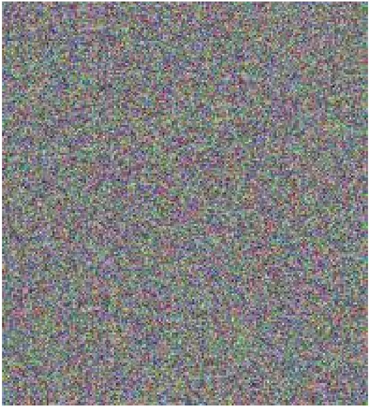
Today's Issues

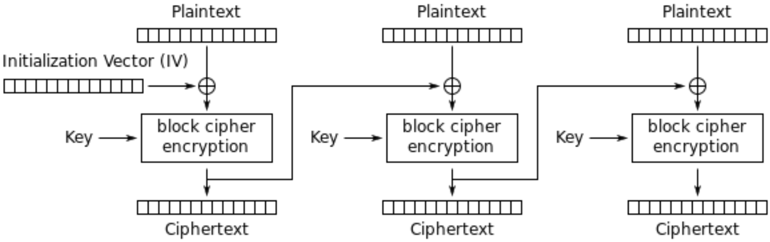
- Mode of operation: ECB
- Goal for security purposes: Pseudo-random result



Today's Issues

- Mode of operation: ECB
- Goal for security purposes: Pseudo-random result
- Other modes of operation: CBC (Cipher Block Chaining)
- A variety of systems are necessary; key exchange





Cipher Block Chaining (CBC) mode encryption

A Brief Overview of Cryptography

OTP

AES: The Advanced Encryption standard
High Level Structure
Rounds

A Historical Transition
Conflicts Throughout History
Cryptography in Our Society

Questions

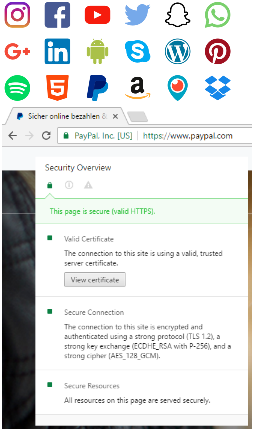
New Possibilities and new Risks

New Possibilities and new Risks

- Technology and social media are becoming ever more linked with our daily lives

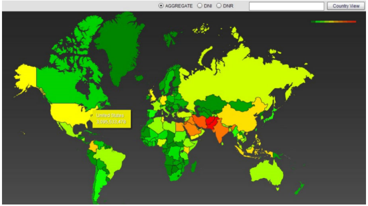
New Possibilities and new Risks

- Technology and social media are becoming ever more linked with our daily lives
- Multiple protocols and algorithms are integral to the security of your data
- Insecure or compromised data can be easily accessed

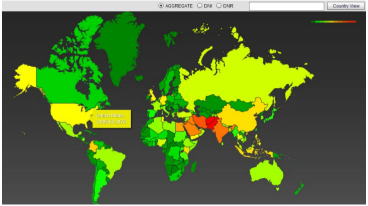


Mass surveillance

Mass surveillance

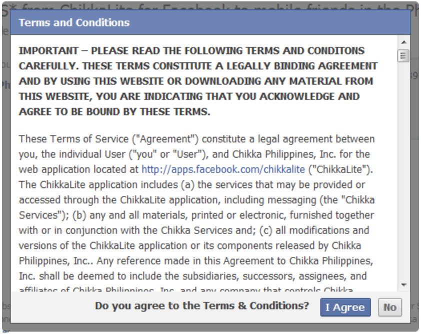


Mass surveillance

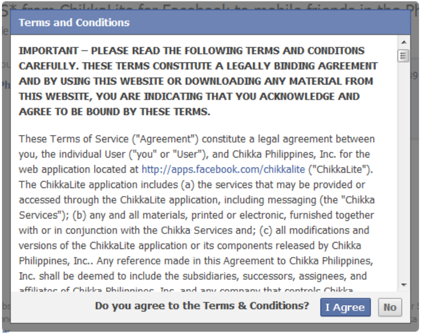


- 3 billion data elements were collected over 30 days in the US alone
- Data collection took place worldwide, including phone call metadata
- Data collection and storage is still active

Privacy: An Outdated Concept?



Privacy: An Outdated Concept?



- Historically academic subject
- Thrust into the public eye through recent revelations
- Highly relevant to the daily lives of regular people for the first time

A Brief Overview of Cryptography

OTP

AES: The Advanced Encryption standard
High Level Structure
Rounds

A Historical Transition
Conflicts Throughout History
Cryptography in Our Society

Questions

Questions

?