CSE 484 / CSE M 584: Computer Security and Privacy

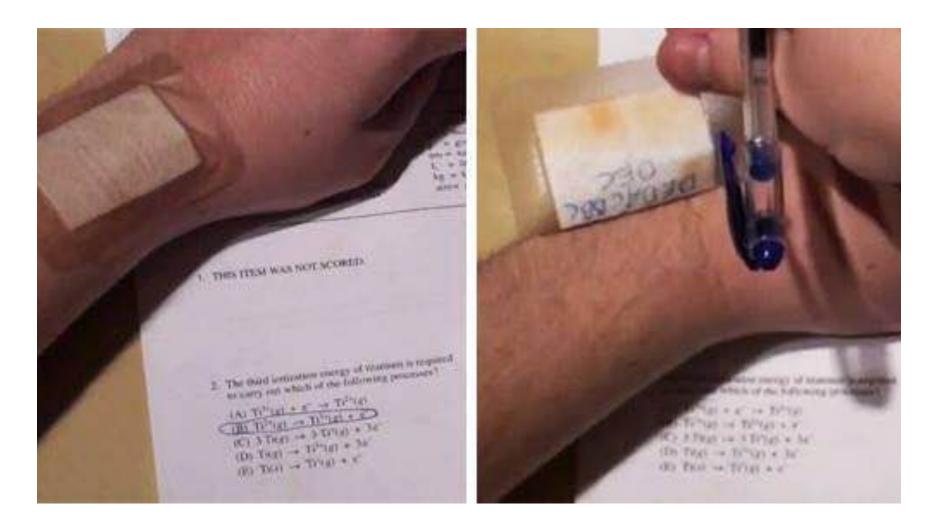
Cryptography: Symmetric Encryption (finish), Hash Functions, Message Authentication Codes

Fall 2016

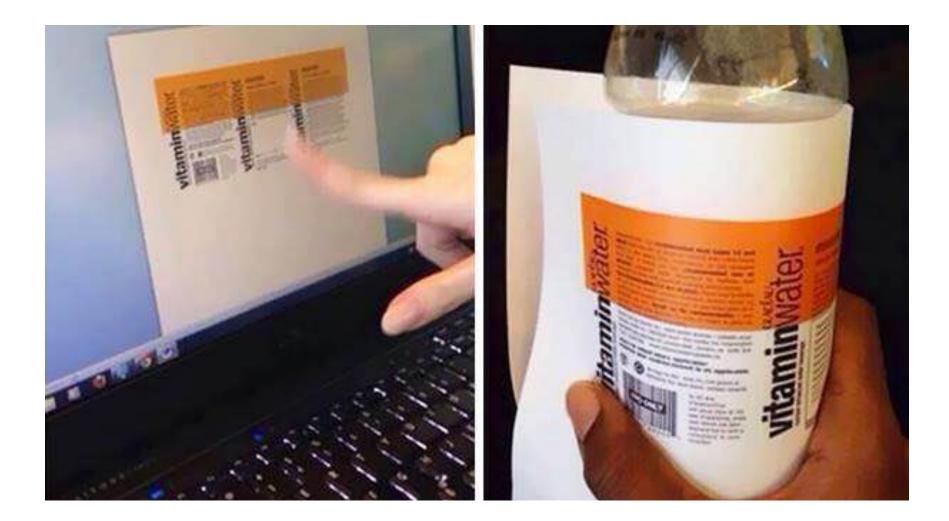
Adam (Ada) Lerner lerner@cs.washington.edu

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

More Cheating



More Cheating



Dirty COW Vulnerability

 Race condition involving memory mapped files which allows user processes to write to root-owned files



Dirty COW Fixed

commit 19be0eaffa3ac7d8eb6784ad9bdbc7d67ed8e619 Author: Linus Torvalds <u>torvalds@linux-foundation.org</u> Date: Thu Oct 13 20:07:36 2016 GMT

This is an ancient bug that was actually attempted to be fixed once (badly) by me eleven years ago in commit 4ceb5db9757a ("Fix get_user_pages() race for write access") but that was then undone due to problems on s390 by commit f33ea7f404e5 ("fix get_user_pages bug").

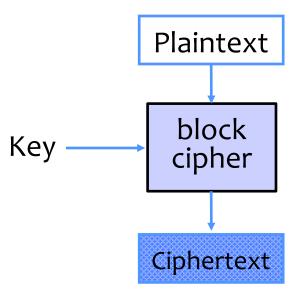
Dirty COW Vulnerability

- madvise(map,100,MADV_DONTNEED)
- write("/proc/self/mem")

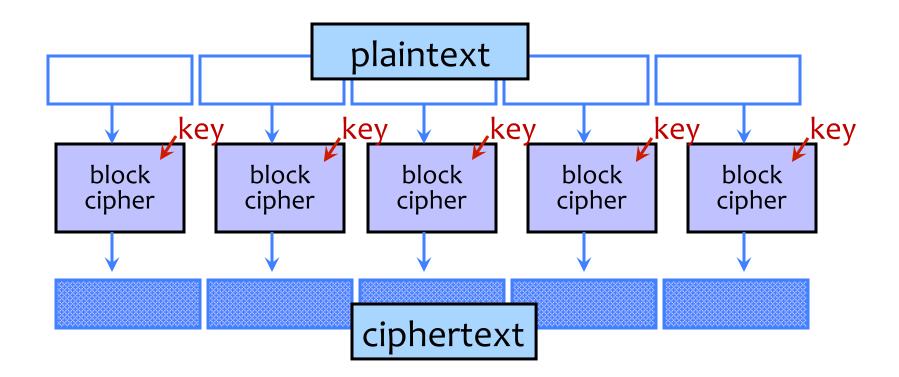
• Eventually writes to a file in the middle of page table updates, causing inappropriate file overwriting.

Recap: Block Ciphers

- Operates on a single chunk ("block") of plaintext
 - For example, 64 bits for DES, 128 bits for AES
 - Each key defines a different permutation
 - Same key is reused for each block (can use short keys)

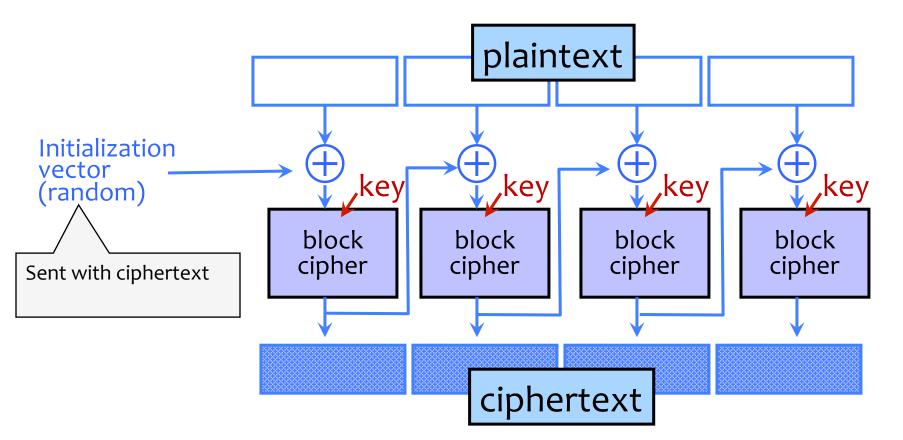


Electronic Code Book (ECB) Mode

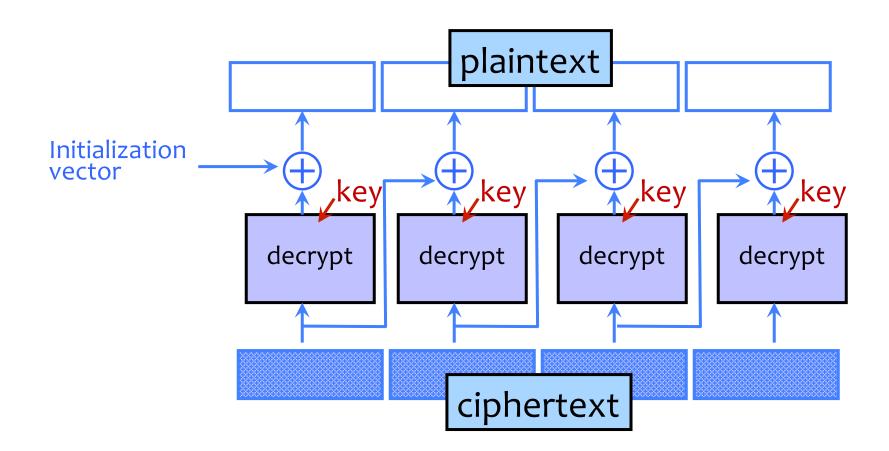


Don't use ECB mode

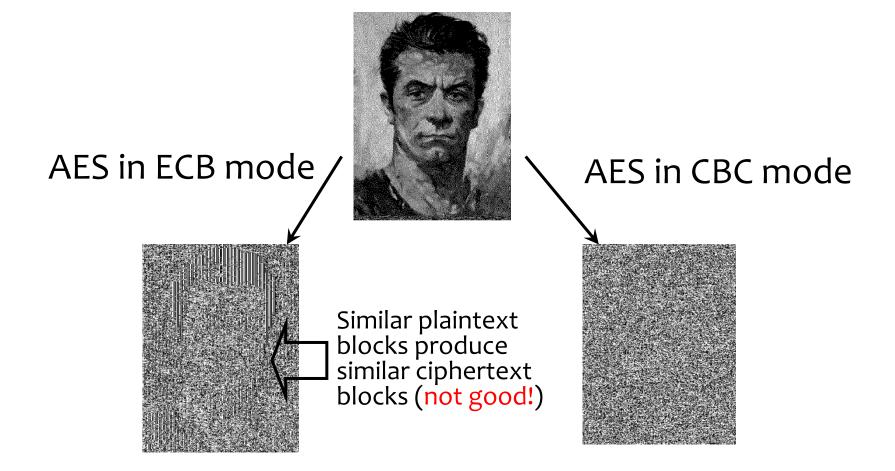
Cipher Block Chaining (CBC) Mode: Encryption



CBC Mode: Decryption



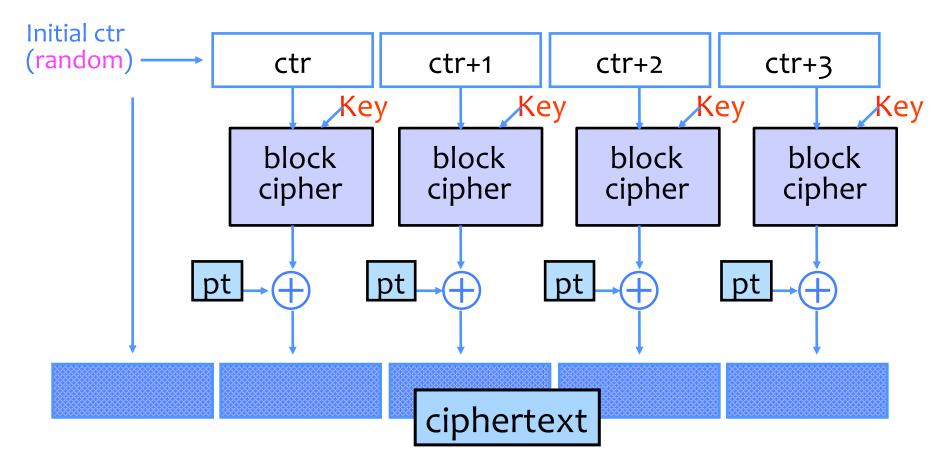
ECB vs. CBC



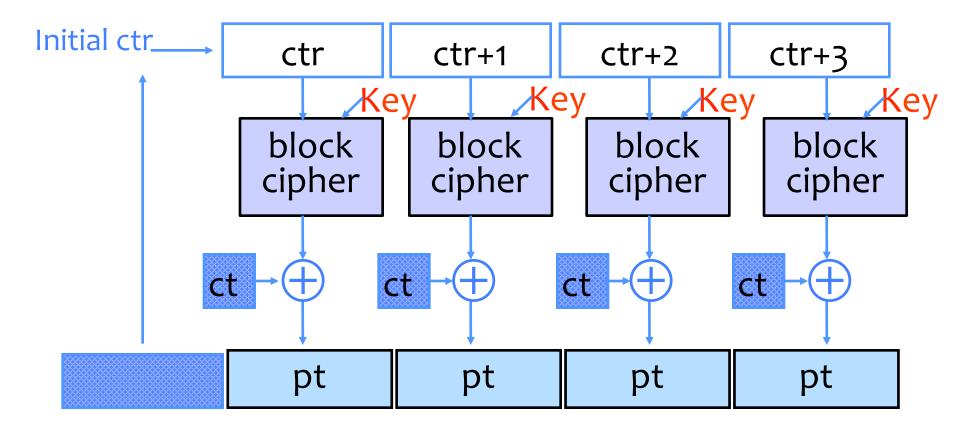
[Picture due to Bart Preneel]

CSE 484 / CSE M 584 - Fall 2016

Counter Mode (CTR): Encryption



Counter Mode (CTR): Decryption



How Can a Cipher Be Attacked?

- Attackers knows ciphertext and encryption algthm
 - What else does the attacker know? Depends on the application in which the cipher is used!
- Ciphertext-only attack
- KPA: Known-plaintext attack (stronger)
 Knows some plaintext-ciphertext pairs
- CPA: Chosen-plaintext attack (even stronger)
 Can obtain ciphertext for any plaintext of his choice
- CCA: Chosen-ciphertext attack (very strong)
 Can decrypt any ciphertext except the target

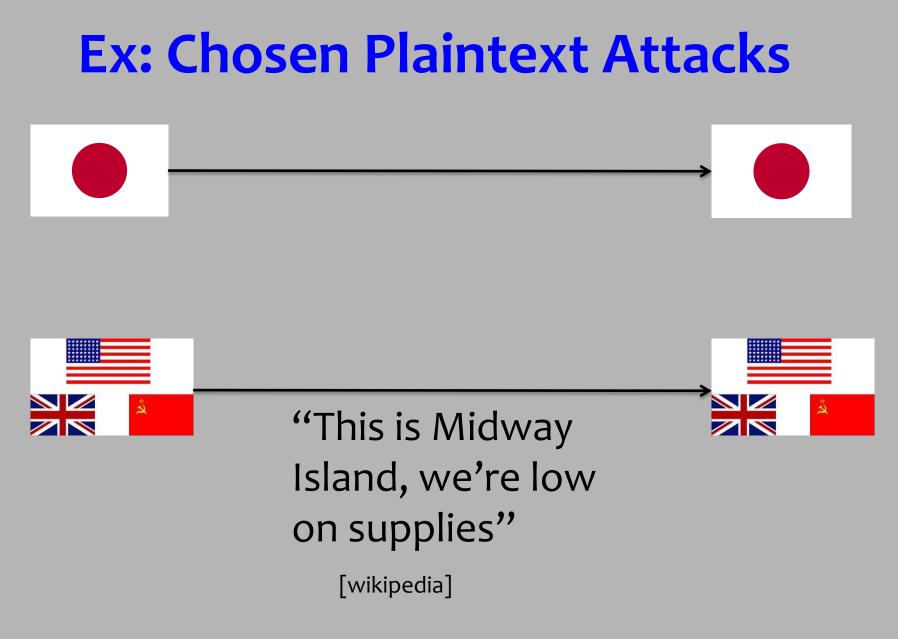
Ex: Chosen Plaintext Attacks

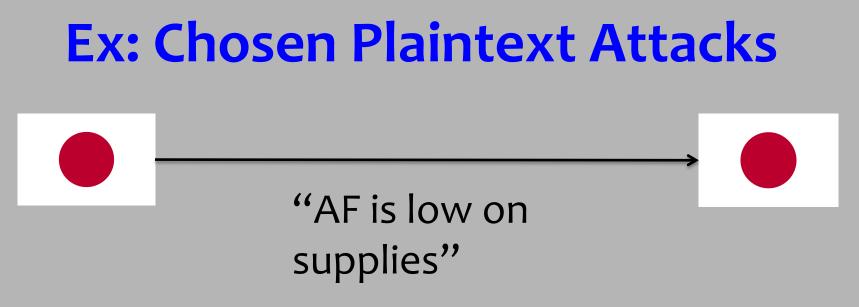
attack on AF"





[wikipedia]









[wikipedia]

Ex: Chosen Plaintext Attack

• When the allies planted mines in the ocean, the German Navy would send messages about those locations to warn their ships.



[wikipedia]

Examples of Chosen Ciphertext Attacks

 Some serious attacks against SSH have been based on Chosen Ciphertext Attacks

• Example: send chosen ciphertext to SSH server, see whether it responds with an error or not.

Examples of Chosen Ciphertext Attacks

- Imagine a system with very few commands, e.g., a military system which responds to the commands ("FIRE") and ("DON'T FIRE"). Try sending ciphertexts and observe in real life whether the weapon fires or not.
- The side effects of the command serve as a "decryption" of your ciphertext.

Very Informal Intuition

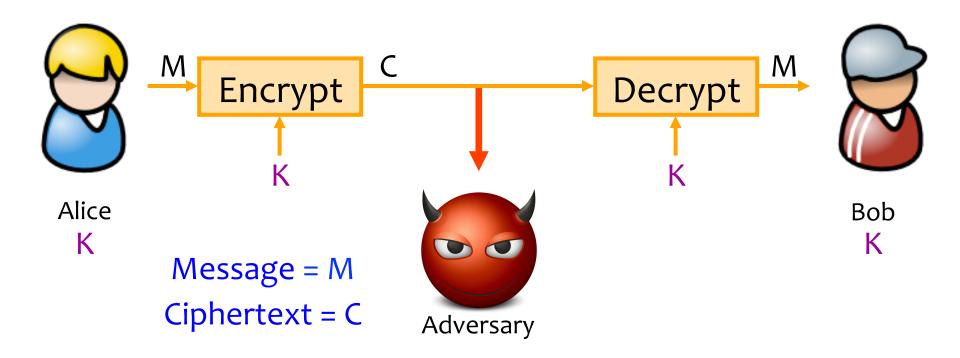
Minimum security requirement for a modern encryption scheme

- Security against chosen-plaintext attack (CPA)
 - Ciphertext leaks no information about the plaintext
 - Even if the attacker correctly guesses the plaintext, he cannot verify his guess
 - Every ciphertext is unique, encrypting same message twice produces completely different ciphertexts

Message Authentication Codes

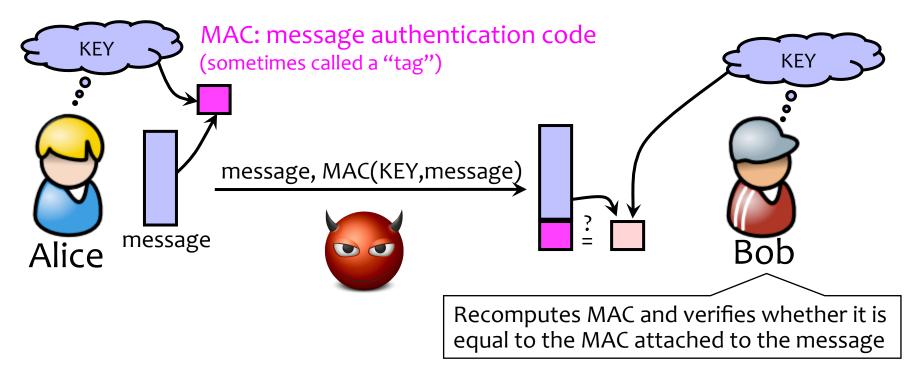
So Far: Achieving Privacy

Encryption schemes: A tool for protecting privacy.



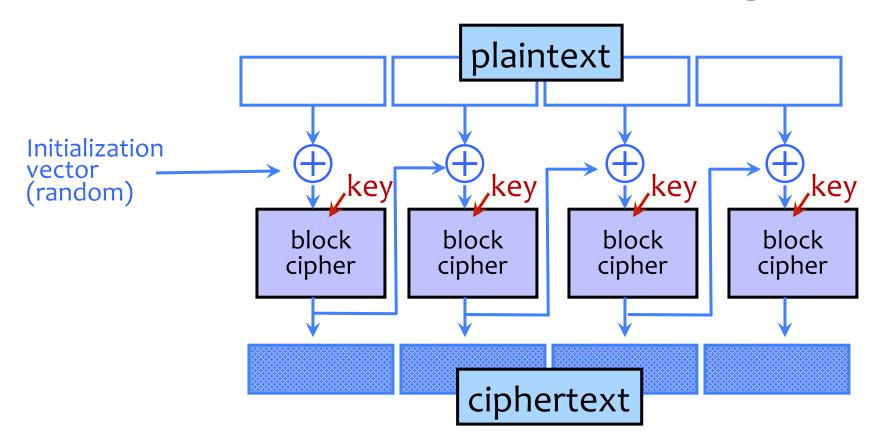
Now: Achieving Integrity

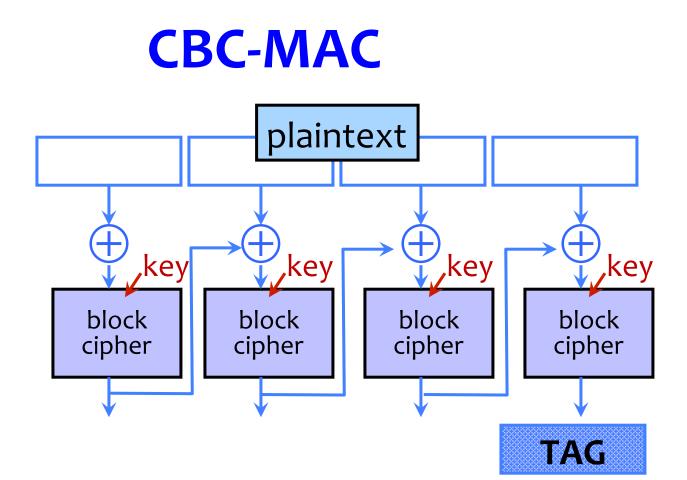
Message authentication schemes: A tool for protecting integrity.

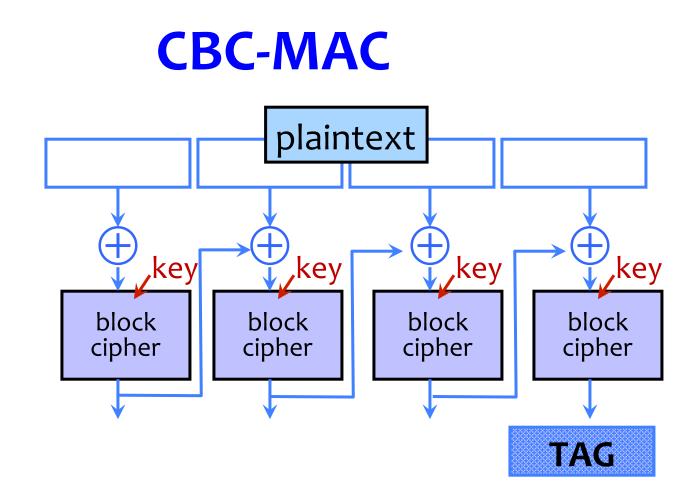


Integrity and authentication: only someone who knows KEY can compute correct MAC for a given message.

Reminder: CBC Mode Encryption





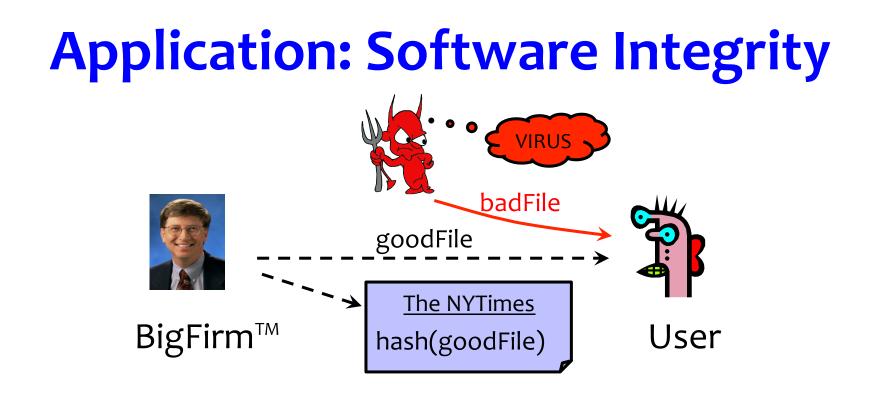


• Not secure when system may MAC messages of different lengths.

Hash Functions

Application: Password Hashing

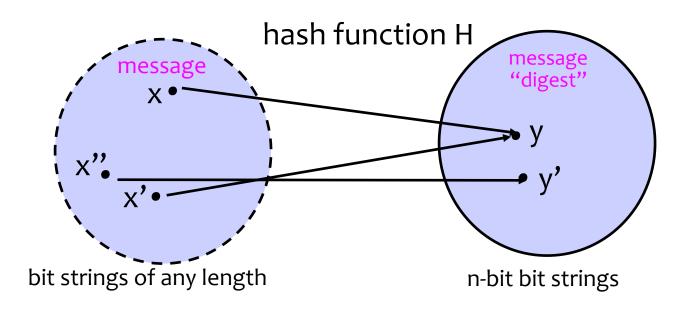
- Instead of user password, store hash(password)
- When user enters a password, compute its hash and compare with the entry in the password file
 - System does not store actual passwords!
 - Cannot go from hash to password!
- Why is hashing better than encryption here?
- Does hashing protect weak, easily guessable passwords?



<u>Goal</u>: Software manufacturer wants to ensure file is received by users without modification.

<u>Idea:</u> given goodFile and hash(goodFile), very hard to find badFile such that hash(goodFile)=hash(badFile)

Hash Functions: Main Idea



Hash function H is a lossy compression function

– Collision: h(x)=h(x') for distinct inputs x, x'

- H(x) should look "random"
 - Every bit equally likely to be 0 or 1
- <u>Cryptographic</u> hash function needs a few properties...

Property 1: One-Way

• The hash should be hard to invert

-"Preimage resistance"

-Let $h(x') = y \in \{0,1\}^n$ for random x'

–Given y, it should be hard to find any x such that h(x)=y

Security Mindset Anecdote

A clever example of a one-way function: phone books.

AT . A LO S A STATE OF	A State
tom 107	
107 TER INC	
123-1932 Harden & Antonio man	
NA - AD TA TANK TANK AND TANK TO AND TANK TO AND TANK	
7-5546 Parket Line Land	1000
1-8201 Tevetin Md & manual & Annual and	
-0410 Tewesi Hansa Gant Terran	
-7215 Jas 14 Deb & Chas 1 to the set of the set	
3856 TFD Management to an	
P200 Thai Jasmine 111 Canta Canta and Canta an	
200 Thairu Hannah In Western	
015 Thakkar Paresh & Panul 39 animum and 978 Post 4129	1
7 86.960 7 86.960 7 86.970 7 86.970 7 86.970 7 96.970 7 96.970 7 96.970 7 96.970 7 96.970 7 96.970 7 96.970 7 96.970 7 96.970 7 97.970 7 97.970 7 97.970 9 7 9 97.970 9 97.970 9 97.970 9 97.970 9 97.970 9 97.970 9 97.970 9 97.970 9 97.970 9 97.970 9 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970 97.970	
14 Thaller Kurt & Carol Stoper La Man. 978 264-4109	
58 Thandapani Suresh 8 Meyer Hill Dr Atn	
58 Tharp Lisa Kauffman 10 Dunham Ln Acton	
7 Thatches Dr Acton	
Patricia 23 Turtle Dr Atn. 978 635-9889 7 Thatcher Photography 5 Till Dr Atn. 978 263-0205 2 Thatcher R 102 Willow W Atn. 978 263-8087	
- Indure Frederic & Lica officiation 978 263-1342	
	-
Wm H Jr 47 North Rd Chel	5
360 Littleton Rd Chel	A
360 Littleton Rd Chel. The Family Eye Care Center 133 Littleton Rd Wsd978 692-14 The Gill Croup 3 Conter 133 Littleton Rd Wsd978 453-55	115
The Gill Group 1 Courthouse Ln Chel	8247
The Family Eye Care Center 133 Littleton Rd Wsd978 453-5 The Gill Group 1 Courthouse Ln Chel	9989
The Mill 481 Great Rd Atn	
The Movement Center Dance Studio 423 Great Rd Atn	1-458
423 Great Rd Atn	6-27
The Pizza Place 210 Boston Rd Chel	12-98
The Total You 326 Great Rd Lttn	592-1
Theall Frank 20 Shaila Av Chel	263
The Total You 326 Great Rd Lttn	392
	0 37
David 89 West St Wsd	809
Daria of fication of Wind	786

Security Mindset Anecdote

A clever example of a one-way function: phone books.

 Hash(name) = Phone number of person with that name

an and a first sub-	A STREET AND
iom the local states of the st	
Teo-The	
CA-SART Section & Antonia and and	States and a second
ST BESS Tatacture Water State	1 24
7-5546 Teversby Vanders & States and States and States	
-0410 Tew John LLC Contract of the Contract of	
-0550 Tewesternet &	
7 B6466 05500 Twoodil Marchine 8 05500 Twoodil Marchine 8 05500 Twoodil Marchine 8 05500 The Shardhow 8 05500 TFC Shardhow 8 05001 TFC Shardhow 8 0502 Thab Kamang Basking Calls 0200 Thai K 137 Case 1 015 Thakkar Paresh 8 0200 Thaik Kar Paresh 8 015 Thakkar Paresh 8 0200 Thaikur Aman 8 015 Thakkar Baresh 8 016 Thaikur Aman 9 017 Thakkar Baresh 8 018 Thaikur Aman 9 019 Thakkar Paresh 8 010 Thakur Aman 9 14 Thalakur Aman 9 14 Thalakur Aman 9 14 Thalakur Aman 9 157 Vijay 8 164 Thanande 9 175 Y78 176 Saman 9 177 Saman 9 178 Saman 9 179 Saman 9 1	
8082 140 Stoney Gate way Co Lee Same tank by Lances 478 57 140	
200 Thairi 12 Cassa La Washing Md Ches.	1
015 Thakkar Paresh & Parel Stand Street	1 2
200 Thakur Aman 3 Trailade Wat 976 392 6	610
14 Thaller Kurt & Carol Slipper La Ata. 978 264-4	40.00
84 Thandapani Suresh 8 Meyer Hill Dr Atn	5000 19567
58 Tharp Lisa Kauffman 10 Dunham Ln Acton. 978 929 56 Thatcher Bruce M 5 Till Dr Atn. 978 633 57 Patricia 23 Turtle Dr Aton. 978 26	-5995
7 Thatcher Photographic Dr Acton	3-0205
2 Thatcher R 102 Willow W Atn. 978 92 Thaure Frederic R 102 Willow W Atn. 978 21	63-8087
Thaure Frederic & Lisa 8 Heather Hill Rd Atn	
VVIII A Jr 47 North Pd Chal	520-2120
WM & Leresa ACculum a chal 9/8	250-2042
The Courtyard Condominium 360 Littleton Rd Chel	8 250-2447
The Family Eve Care Center 133 Littleton Rd Wsd97	8 692-1400
The Gill Group 1 Courthouse Ln Chel	78 453-5115
The Gutierrez Co 2 Technology Pk Dr Wsd	78 263-9989
The Mill 481 Great Rd Atn	10 203 110
The Movement Center Dance Studio 423 Great Rd Atn	978 264-458
423 Great Rd Atn	978 256-27
The Pizza Place 210 Boston Rd Chel The Stone Yard 2 Spectacle Pond Rd Lttn The Total You 326 Great Rd Lttn The Total You 326 Great Rd Lttn	978742-98
The stone varu / Speciacle Pollu itu La	078 400 0
The Total You 326 Great Rd Lttn The Whole Body Studio 187 Littleton Rd Wsd	
Thoateo III Brit LIIILE 200 Condia	970 97
Theide D 80 West St Wsd	978 39
There D by West St Wisd	978 6
Theide D 89 West St Wsd David 89 West St Wsd	078 6

Security Mindset Anecdote

- Easy to compute forward (phonebook is alphabetical)
- Hard to invert backward (must search n/2 pages on average to find person by phone number)

AT A LOCAL DISCOURSE OF A DESCRIPTION OF A DESCRIPTIONO OF A DESCRIPTION OF A DESCRIPANTE A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A	Sec. 1
som	
AND TOT	
23-1922 Reliant & Annual Constant	
SF ACCOUNTS AND	
7-5546 Ferences Annual Land	
-B201 Terron LLC Contained and Annual	
-0410 Tewstill Harden & Gall & Annual and an an an and an	
0501 TFC Studio tel so a ches a menter a menter	1
8082 148 Stoney Gate way Call and Stoney Gate Way Cartan	
200 Thai K 12 Case 1n Westing to Class	
015 Thakkar Paresh & Parul to Atlanta 976 854 8185	1
200 Thakur Aman 3 Traitaide We Water 978 392 8810	
3 Rescale Texture Rescale Rescale <t< td=""><td></td></t<>	
58 Tharp Lisa Kauffman Meyer Hill Dr Atn	
6 Thatcher Bruce M 5 Till Dr Atn	
9 Patricia 23 Turtle Dr Attn	ő
2 Thatcher R 102 Willow W Atn. 978 263-800 Thaure Frederic 8	87
Thayer Kent & Astrid 45 Data wills Rd Chel	260
VVIII D JF 47 North Pd Chal	1730
Wm & Teresa 46 Sylvan Av Chel	
360 Littleton Rd Chel	-2447
The Family Eye Care Center 133 Littleton Rd Wsd978 692	2-1400
The Gill Group 1 Courthouse Ln Chel	9-8247
The Gutterrez Co 2 Technology Pk Dr Wsd	63-9989
The Mill 481 Great Rd Atn	
422 Great Pd Ata	264-430
423 Great Rd Atn	742-98
The Stone Vard 2 Spectacle Pond Rd Lttn	A86-8
The Total You 326 Great Rd Ittn.	9 692-1
The Whole Body Studio 187 Littleton Rd Wsd	18 251-
The Whole Body Stadio to chai	79 263
Theall Frank 20 Shella Av Chel	70 202
Theall Frank 20 Sheila Av Chel	070 30
Theide D 89 West St Wsd David 89 West St Wsd	918 37
David 89 West St Wsd	978 0
the second of the second secon	078 6



10/26/16

Property 2: Collision Resistance

• Should be hard to find x≠x' such that h(x)=h(x')

Birthday Paradox

- Expect birthday "collision" half the time with a room of only 23 people.
 - Approximate: 50% probability = sqrt(365).
- Why is this important for cryptography?
 - 2¹²⁸ different 128-bit values
 - Pick one value at random. To exhaustively search for this value requires trying on average 2¹²⁷ values.
 - Expect "collision" after selecting approximately 2⁶⁴ random values.
 - 64 bits of security against collision attacks, not 128 bits.

Property 2: Collision Resistance

- Should be hard to find x≠x' such that h(x)=h(x')
- Birthday paradox (informal)
 - Let t be the number of values x,x',x''... we need to look at before finding the first pair x,x' s.t. h(x)=h(x')
 - What is probability of collision for each **pair** x,x'? $1/2^n$
 - How many **pairs** would we need to look at before finding the first collision? O(2ⁿ)
 - How many pairs x,x' total? Choose(t,2)=t(t-1)/2 ~ $O(t^2)$
 - What is t, the **number** of values we need to look at? $2^{n/2}$
- Brute-force collision search is only O(2^{n/2}), not O(2ⁿ)
 For SHA-1, this means O(2⁸⁰) vs. O(2¹⁶⁰)

Property 2: Collision Resistance

- Should be hard to find $x \neq x'$ such that h(x)=h(x')
- Birthday paradox means that brute-force collision search is only O(2^{n/2}), not O(2ⁿ)

- For SHA-1, this means $O(2^{80})$ vs. $O(2^{160})$

Property 3: Weak Collision Resistance

- Given randomly chosen x, hard to find x' such that h(x)=h(x')
 - Attacker must find collision for a <u>specific</u> x. By contrast, to break collision resistance it is enough to find <u>any</u> collision.
 - Brute-force attack requires O(2ⁿ) time
- Weak collision resistance does <u>not</u> imply collision resistance.

Properties of a Cryptographic Hash Function

- One-wayness
 Given h(x)...
- Collision resistance
 Hard to find...
- Weak collision resistance
 Hard to find...

Properties of a Cryptographic Hash Function

- One-wayness
 Given h(x): hard to find x
- Collision resistance
 Hard to find x ≠ x' s.t. h(x) == h(x')
- Weak collision resistance

 Hard to find x ≠ x' s.t. h(x) == h(x')
 for specific, random x