Crypto Primitives

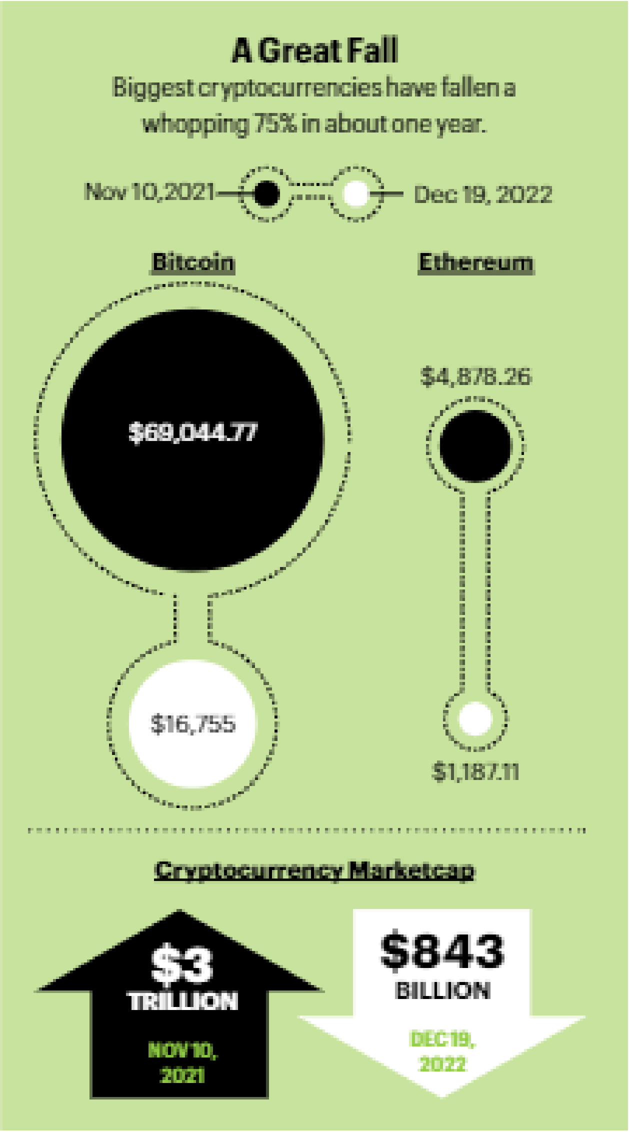
V. Balasubramanian
Professor, Department of CSE
(Cyber Security)
Rajalakshmi Engineering College

Outline

- Introduction
- Genesis of Blockchain
- Cryptographic Hash Functions
- Characteristics of Blockchain
- Digital Signature
- Smart Contract

Jan 2023

- Bitcoin miners—the people who run computations in order to earn new bitcoins—are using approximately half of 1% of the world’s energy output. [running for 13 years]
- Digiconomist, a website that tracks resources used
- Bitcoin -131 tera watt hours (TWh) of electricity [Argentina]
- Ethereum -78TWh per year [Chile]
- Dogecoin - 3TWh per year [Montenegro Balkan Country]



Indians 6 Lakh crores
$75 Billion

Contd…

- Increased carbon emissions and contributes to climate change.
- September 2022, Ethereum - Merge, changing its proof of work to the less-energy-intensive proof of stake. Electricity demand reduced by 99%.
- The main barrier is cultural: Bitcoin is fiercely against even tiny changes to the monetary policy

Contd…

- Proposal Limiting Proof-of-Work Is Rejected in EU Parliament Committee Vote on March 14, 2022 [27 countries]
- Sweden Prefers Steel Over Bitcoin Miners as Power Gets Scarce [they have hydro power]
- New York Signs Two-Year Crypto Mining Moratorium Into Law Nov 22.
- China banned Bitcoin in 2021, but miners moved to Kazakhstan.
- Ban on PoW - free speech implications

Radical New Thinking

- Extraordinary circumstances call for radical thinking (chaos and confusion)
- Financial Crisis 2008
- Counter party risk – accumulating risk both collapse [party a & b, if other not fulfilling]
- Double spending: resources committed for one domain can not be committed for another domain
- Bundling: High risk Mortgages + low risk public stock

Events

- The bankruptcy of Lehman Brothers on September 15, 2008 chapter 11 petition - more than US$600 billion in assets
- Sept. 16, the Federal Reserve deemed AIG systemically important to the global financial system and provided the company with an $85-billion
- Sep 25, Washington Mutual was a conservative savings and loan bank. In 2008, it became the largest failed bank in U.S. history. By the end of 2007, WaMu had more than 43,000 employees, 2,200 branch offices in 15 states, and $188.3 billion in deposits

Events

- Sept. 15, 2008, Lehman Brothers bankruptcy. WaMu depositors panicked upon hearing this. They withdrew $16.7 billion out of their savings and checking accounts over the next 10 days
- Sep 29 The Dow bounced around 11,000 until September 29, 2008, when the Senate voted against the bailout bill. The Dow lost 777.68 points during intraday trading. Global markets also panicked:
- Sensex had dropped from around 20,465 points to 9716 points

Events

- On October 3, 2008, President George W. Bush signed the $700 billion Emergency Economic Stabilization Act (EESA)
- Severe impact on the people. By and large public is affected and lost faith in Financial Institutions.
- Whole system collapsed because of centralized nature.

Nov 2, 2008

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Genesis Block Jan 3, 2009

- Genesis Block
- ***The Times 03/Jan/2009 Chancellor on brink of second bailout for banks***

Crypto Primitives

```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

Crypto Primitives

THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Israel prepares to send tanks and troops into Gaza

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salmon Rushdie I Won't Marry Again

Giant Killing? Guide to the FA Cup Third Round

Chancellor on brink of second bailout for banks

Billio[illegible] may be needed as lending squeeze tightens

99p

News

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offiering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed gurantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels
Business, page 47

Gerald Cotton Quadriga

A crypto exchange may have lost $145 million after its CE(suddenly died

By Daniel Shane, CNN Business

Updated 0251 GMT (1051 HKT) February 6, 2019

TOP STORIES

Steve Harvey
Miss Univers

A wildlife cor
mauled by he

A coding error led to $30 million in ethereum being stolen

Brewer’s Theorem

- CAP – Consistency, Availability and Paritition tolerance
- Nakomato - Eventual consistency


I LOST MY I.D. BADGE.
REPORT TO THE SECURITY OFFICE AND GET A NEW ONE.
HOLD IT! WHERE DO YOU THINK YOU'RE GOING?
TO THE SECURITY OFFICE?
NO ONE IS ALLOWED PAST THIS DESK WITHOUT AN I.D. BADGE.
OKAY...HOW DO I GO TO THE SECURITY OFFICE IF I CAN'T GO TO THE SECURITY OFFICE?
GOOD QUESTION. I GUESS YOU'LL HAVE TO SNEAK PAST ME.
LOOK OVER THERE! IT'S AN ANGEL, AND SHE'S GIVING AWAY FREE BACON!
WELL, WELL; IT SEEMS I'VE FOUND A WORTHY ADVERSARY.
E-mail: SCOTTADAMS@AOL.COM
© 2004 Scott Adams, Inc./Dist. by UFS, Inc.
www.dilbert.com

Blockchain

Blockchain technology is a digital innovation that has the potential to significantly impact trusted computing activities and therefore cybersecurity concerns as a whole.

Attractive properties of Blockchain

- Log of data with digital signature
- Immutable (once written – cryptographically hard to remove from the log)
- Cryptographically secure – privacy preserving
- Provides a basis for trusted computing on top of which applications can be built

Algebraic Structure

- Ease of Computation Depends on the representation
- Depends on the operation

Ease/Speed of Operation Depends on the Representation

- viii * xvi = cxxviii
- $8 * 16 = 128$
- $2^3 * 2^4 = 2^7$

- viii + xvi = xxiv
- $8 + 16 = 24$
- $2^3 + 2^4 = 2^3.3$

- viii < ix is true
- $8 < 9$ is true
- $2^3 < 3^2$ is true

Is There a Representation Where all Common Operations are FAST?

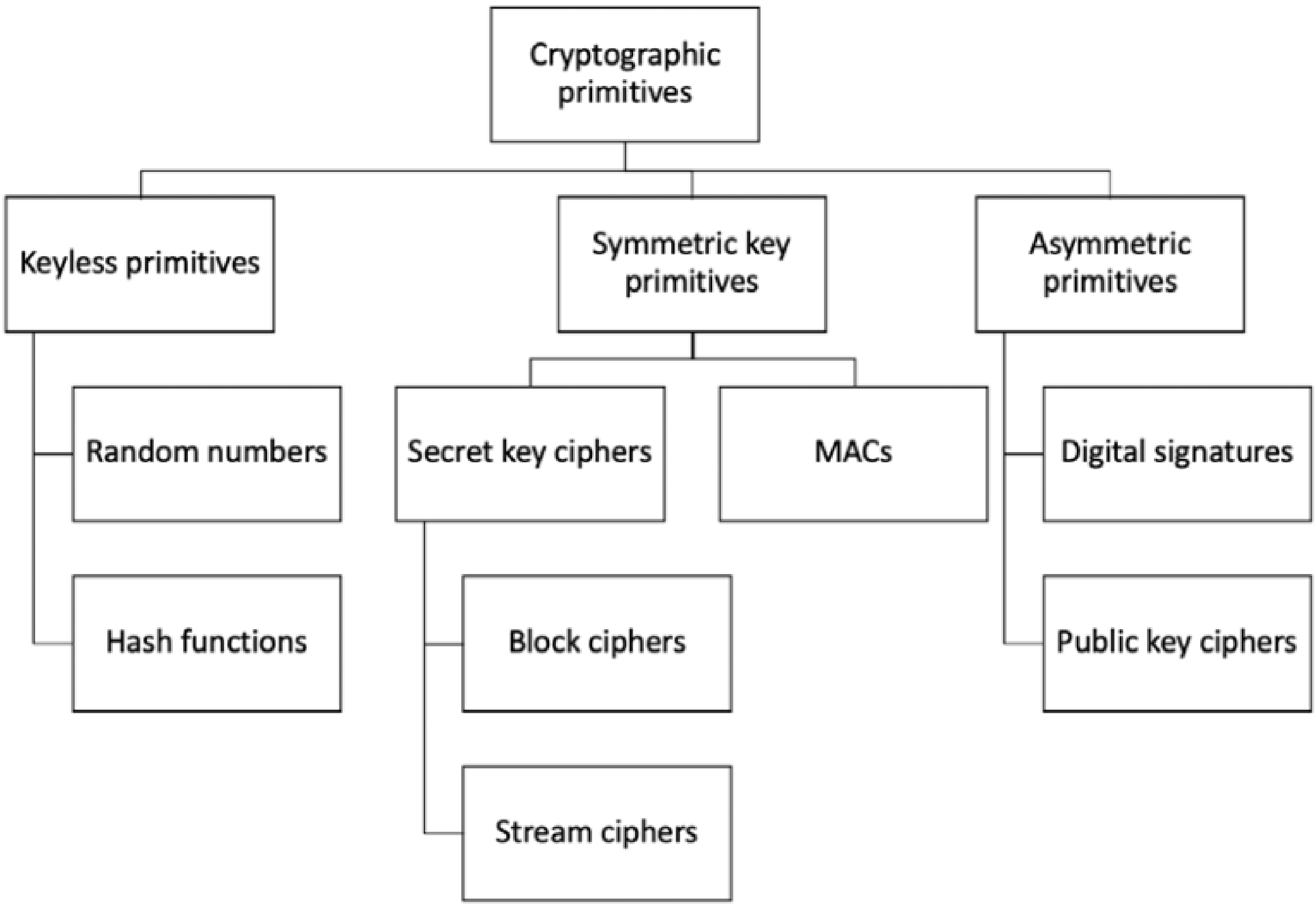
Not Easy!

- Addition (+)
- Comparison (<)
- Multiplication (*)

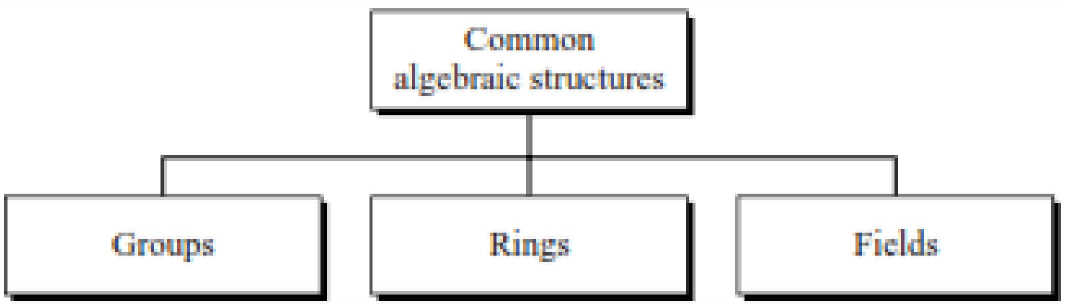
Why is the Decimal System Popular?

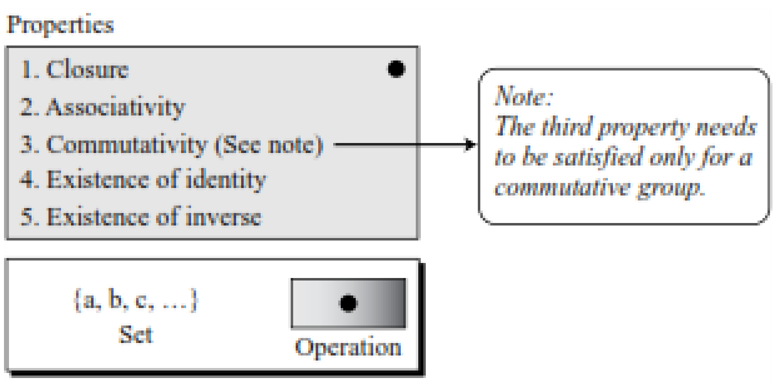
	Addition	Multiplication	Comparison
ROMAN	SLOW	SLOW	SLOW
DECIMAL	**FAST**	MEDIUM	**FAST**
PRIME PRODUCT	SLOW	**FAST**	MEDIUM
RESIDUE SYSTEM	**FAST**	**FAST**	MEDIUM

Crypto Primitives

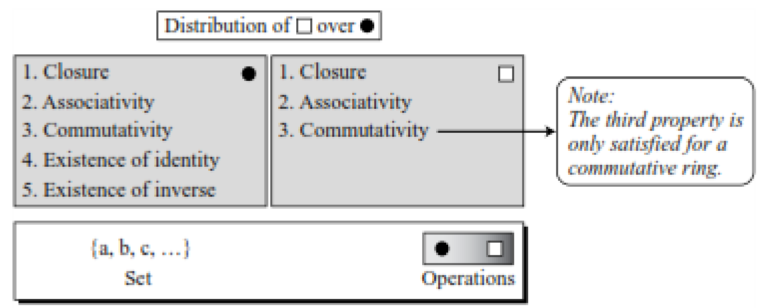


Common Algrebraic structures



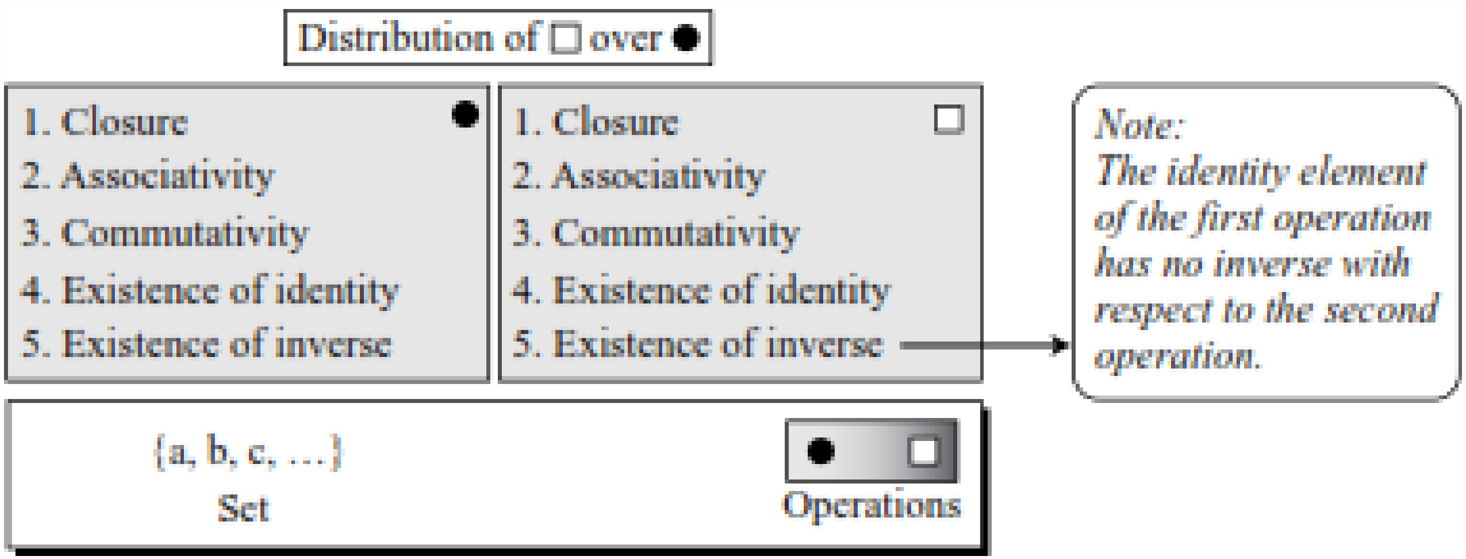


Group



Ring

Field



Field

Addition/subtraction in GF(2) is the same as the XOR operation; multiplication/division is the same as the AND operation.

Prime Fields (p^n) where n=1

GF(5)

{0, 1, 2, 3, 4} + ×

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Addition

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication

Additive inverse

a	0	1	2	3	4
$-a$	0	4	3	2	1

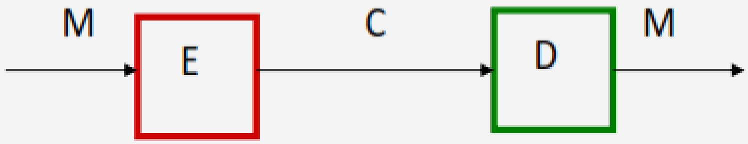
a	0	1	2	3	4
a^{-1}	—	1	3	2	4

Multiplicative inverse

Contd…

Algebraic Structure	*Supported Typical Operations*	*Supported Typical Sets of Integers*
Group	$(+\ -)$ or $(\times\ \div)$	$\mathbf{Z}_n$ or $\mathbf{Z}_n{}^*$
Ring	$(+\ -)$ and $(\times)$	$\mathbf{Z}$
Field	$(+\ -)$ and $(\times\ \div)$	$\mathbf{Z}_p$

Encryption / Decryption



The following identity must hold true:

$D(C) = M$, where $C = E(M)$

$M = D(E(M))$

$K_1 = K_2$.

. $K_1 \,!= K_2$

Keyless

Linear Congruential Generators

A widely used technique for pseudorandom number generation is an algorithm first proposed by Lehmer [LEHM51], which is known as the linear congruential method. The algorithm is parameterized with four numbers, as follows:

m	the modulus	$m > 0$
a	the multiplier	$0 < a < m$
c	the increment	$0 \le c < m$
X_0	the starting value, or seed	$0 \le X_0 < m$

The sequence of random numbers $\{X_n\}$ is obtained via the following iterative equation:

$$X_{n+1} = (aX_n + c) \bmod m$$

a=7, $c = 0$, $m = 32$, and $X_0 = 1$

$X_{n+1} = (aX_0 + c) mod\ m$

$X_1 = (7 * 1 + 0) mod\ 32 = 7$

$X_2 = (7 * 7 + 0) mod\ 32 = 17$

$X_3 = (7 * 17 + 0) mod\ 32 = 23$

$X_4 = (7 * 23 + 0) mod\ 32 = 1$

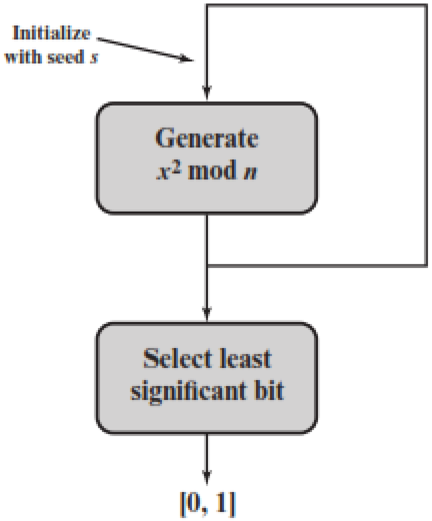
$X_5 = (7 * 1 + 0) mod\ 32 = 7$

Blum Blum Shub

$p \equiv q \equiv 3 \pmod 4$ $\qquad n = p \times q$

choose a random number s, such that s is relatively prime to n;

```
    X0 = s^2 mod n
for i = 1 to ∞
    Xi = (Xi-1)^2 mod n
    Bi = Xi mod 2
```



Here, *n = 192649 = 383 * 503, and the seed s = 101355*

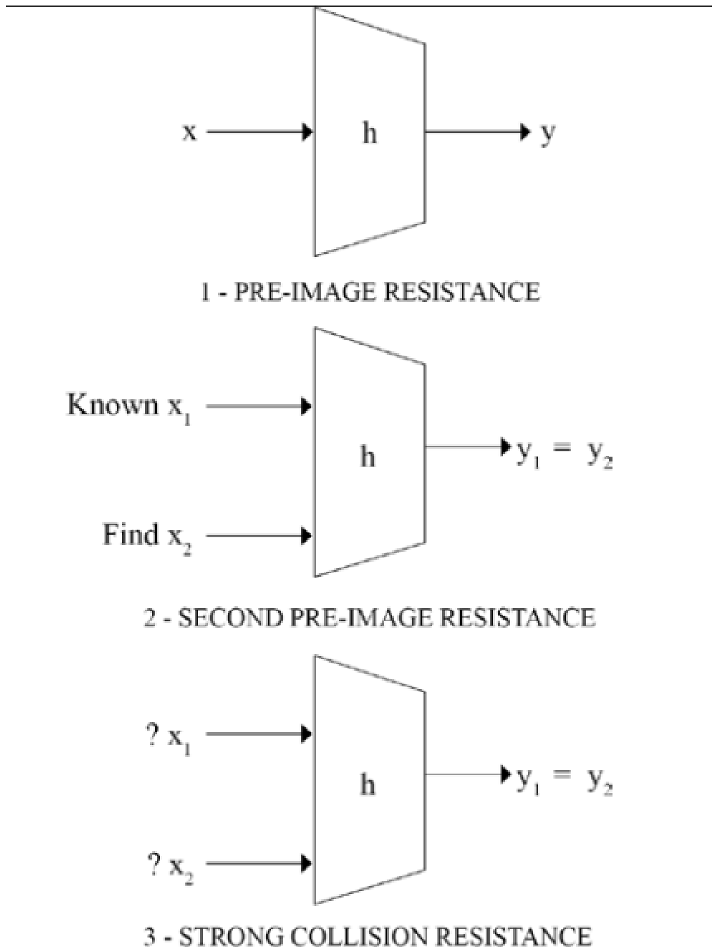
i	X_i	B_i
0	20749	
1	143135	1
2	177671	1
3	97048	0
4	89992	0
5	174051	1

Hash Algorithms

Properties of Hash Functions

1. **Arbitrary message size** $h(x)$ can be applied to messages x of any size.
2. **Fixed output length** $h(x)$ produces a hash value z of fixed length.
3. **Efficiency** $h(x)$ is relatively easy to compute.
4. **Preimage resistance** For a given output z, it is impossible to find any input x such that $h(x) = z$, i.e, $h(x)$ is one-way.
5. **Second preimage resistance** Given x_1, and thus $h(x_1)$, it is computationally infeasible to find any x_2 such that $h(x_1) = h(x_2)$.
6. **Collision resistance** It is computationally infeasible to find any pairs $x_1 \neq x_2$ such that $h(x_1) = h(x_2)$.

Properties

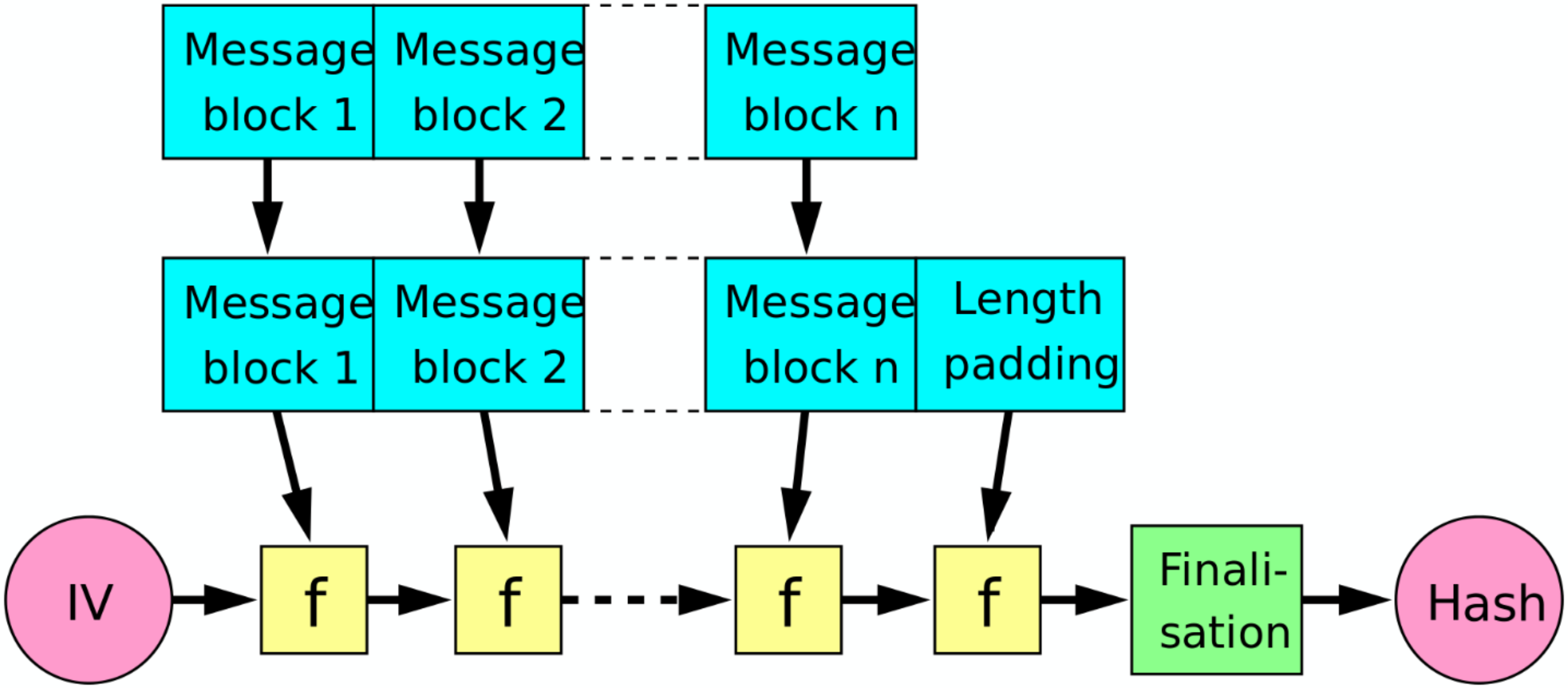

x
h
y
1 - PRE-IMAGE RESISTANCE
Known x_1
Find x_2
h
$y_1 = y_2$
2 - SECOND PRE-IMAGE RESISTANCE
? x_1
? x_2
h
$y_1 = y_2$
3 - STRONG COLLISION RESISTANCE

Examples

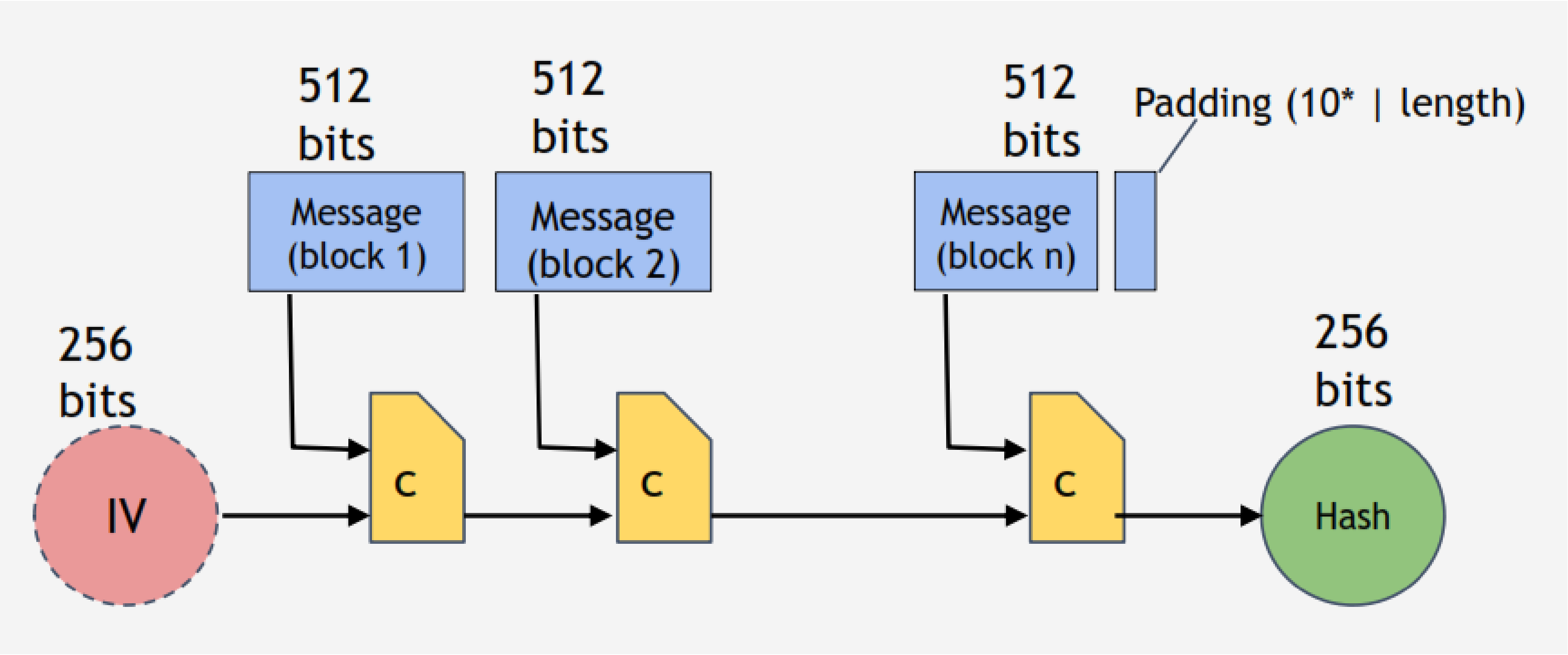
- MD5 128 Bit
- SHA -0/1 160 Bit
- RACE Integrity Primitives Evaluation Message Digest 128/160/256/320

- The SHA-256 algorithm is used in Bitcoin's PoW algorithm

Merkle Function



Collision Resistant



Crypto Tools used

- Public key cryptography - Bitcoin uses public key cryptography to handle transactions.
- Hash functions. Bitcoin uses hash functions to secure the information in the blockchain.
- Symmetric key cryptography. Bitcoin uses symmetric encryption to protect the private keys in a user’s wallet.

Public Key Algorithms

- **Integer factorization.** These algorithms are based on the difficulty of factoring large integers. The most important example is RSA, introduced in 1977 (Rivest et al., 1978).
- **Discrete logarithm (DL).** Based on the intractability of the discrete logarithm problem on finite cyclic groups. It was introduced in 1976 by Diffie and Hellman for their proposed key exchange algorithm (Diffie and Hellman, 1976).
- **Elliptic curve (EC).** Based on the difficulty of computing the generalized logarithm problem on an elliptic curve. It was introduced in 1985. Despite its technical advantages, adoption has been somewhat limited by the patents covering it.

PKI

EXAMPLE RSA Cryptosystem

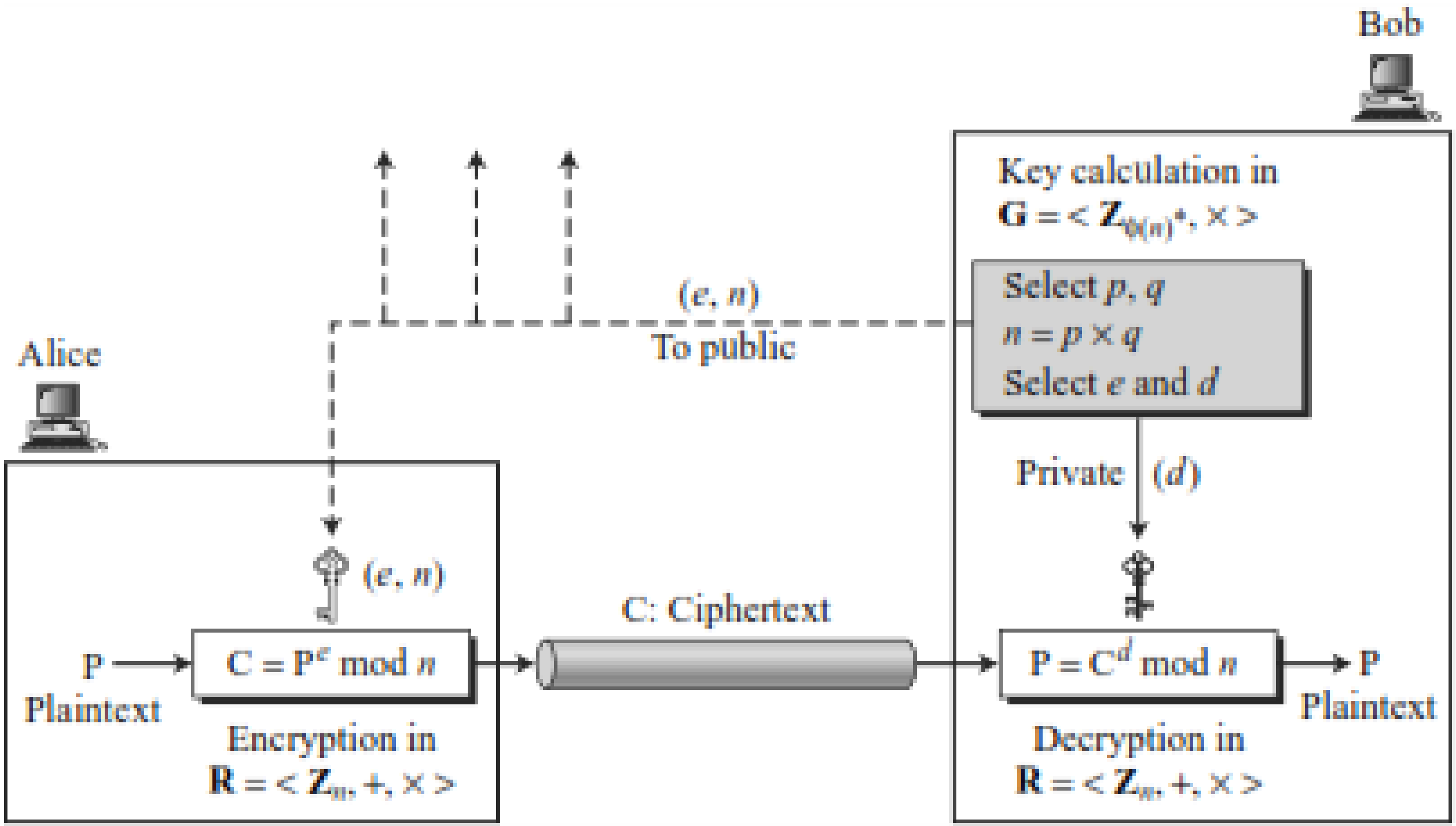
R_1 : Product of Primes

R_2 : Decimal

E_K : Modular Exponentiation

$$m^e \bmod K$$

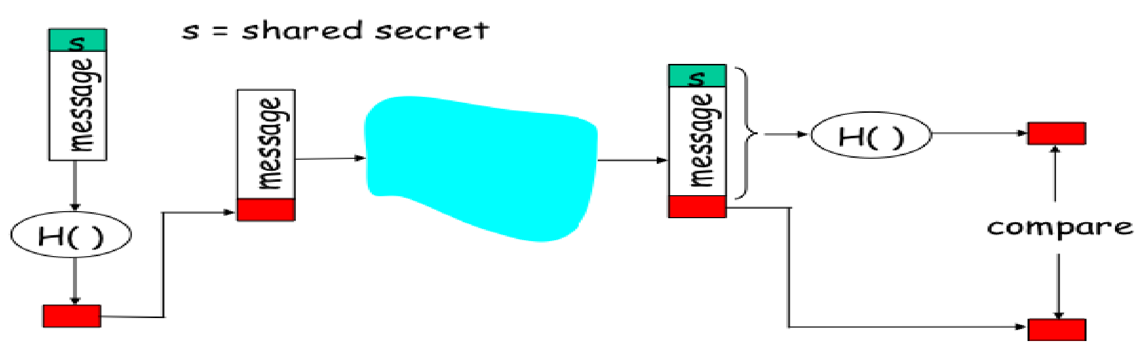
RSA


Bob
Key calculation in
$\mathbf{G} = < \mathbf{Z}_{\phi(n)}^*, \times >$
Select p, q
$n = p \times q$
Select e and d
(e, n)
To public
Private (d)
Alice
(e, n)
C: Ciphertext
P
Plaintext
$C = P^e \bmod n$
Encryption in
$\mathbf{R} = < \mathbf{Z}_n, +, \times >$
$P = C^d \bmod n$
P
Plaintext
Decryption in
$\mathbf{R} = < \mathbf{Z}_n, +, \times >$

Message Authentication

- A Message Authentication Code (MAC), also known as a cryptographic checksum or a keyed hash function, is widely used in practice.

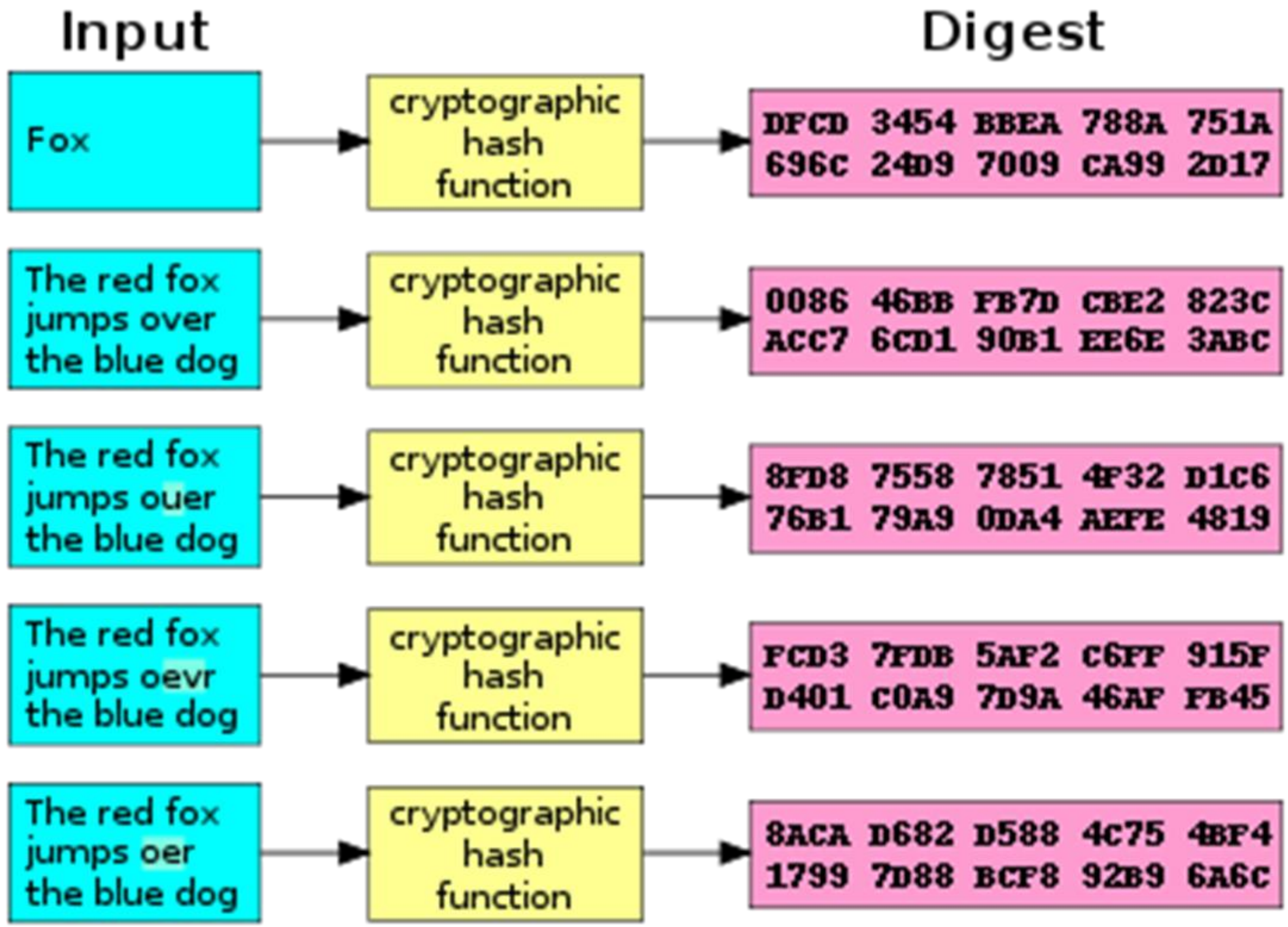
Hash-Based Message Authentication Code (HMAC)



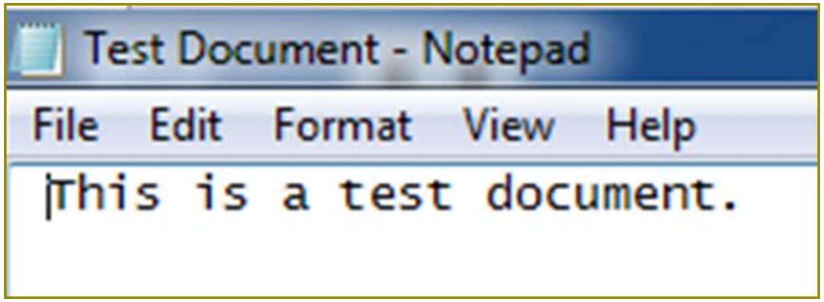
- ***Authenticates sender***
- ***Verifies message integrity***
- No encryption!
- Also called “keyed hash”

Tools

- WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor
- Openssl
- Boringssl – Google
- S2n - Amazon



Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C



Hash Values of above document	
MD5 Hash (128 bit)	7EB7781398042342E50BC37E93CCC854
SHA 1 **(160 bit)**	**CB80455993111C16FD13E70125852AEFC91 1F31E**

SHA 256 **(256 bit)**	**EC7F4FEDDD1C1349AD5A4D9C913A5C4E 21A226E6719CD1B2805225DF7075D22F**

Evidence Preserving

- Examples of hash functions are MD5 and SHA-1, SHA-2.
- MD5 was developed by Professor Ronald L. Rivest of MIT.
- The MD5 algorithm takes as input a message of arbitrary length and produces as output a 128-bit fingerprint of the input.

Example

=

79054025
255fb1a2
6e4bc422
aef54eb4

MD5

MD5 Collision

d131dd02c5e6eec4693d9a0698aff95c2fcab58712467eab4004583eb8fb7f89
55ad340609f4b30283e488832571415a085125e8f7cdc99fd91dbdf280373c5b
d8823e3156348f5bae6dacd436c919c6dd53e2b487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080a80d1ec69821bcb6a8839396f9652b6ff72a70

and

d131dd02c5e6eec4693d9a0698aff95c2fcab50712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325f1415a085125e8f7cdc99fd91dbd7280373c5b
d8823e3156348f5bae6dacd436c919c6dd53e23487da03fd02396306d248cda0
e99f33420f577ee8ce54b670802 80d1ec69821bcb6a8839396f965ab6ff72a70


A 30-23-12
A 30-23-05
ENTERING VEHICLE CONTROL ZONE

SHA Attack

- Here are some numbers that give a sense of how large scale this computation was:

  Nine quintillion (9,223,372,036,854,775,808) SHA1 computations in total
- 6,500 years of CPU computation to complete the attack first phase
- 110 years of GPU computation to complete the second phase
- https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

Properties

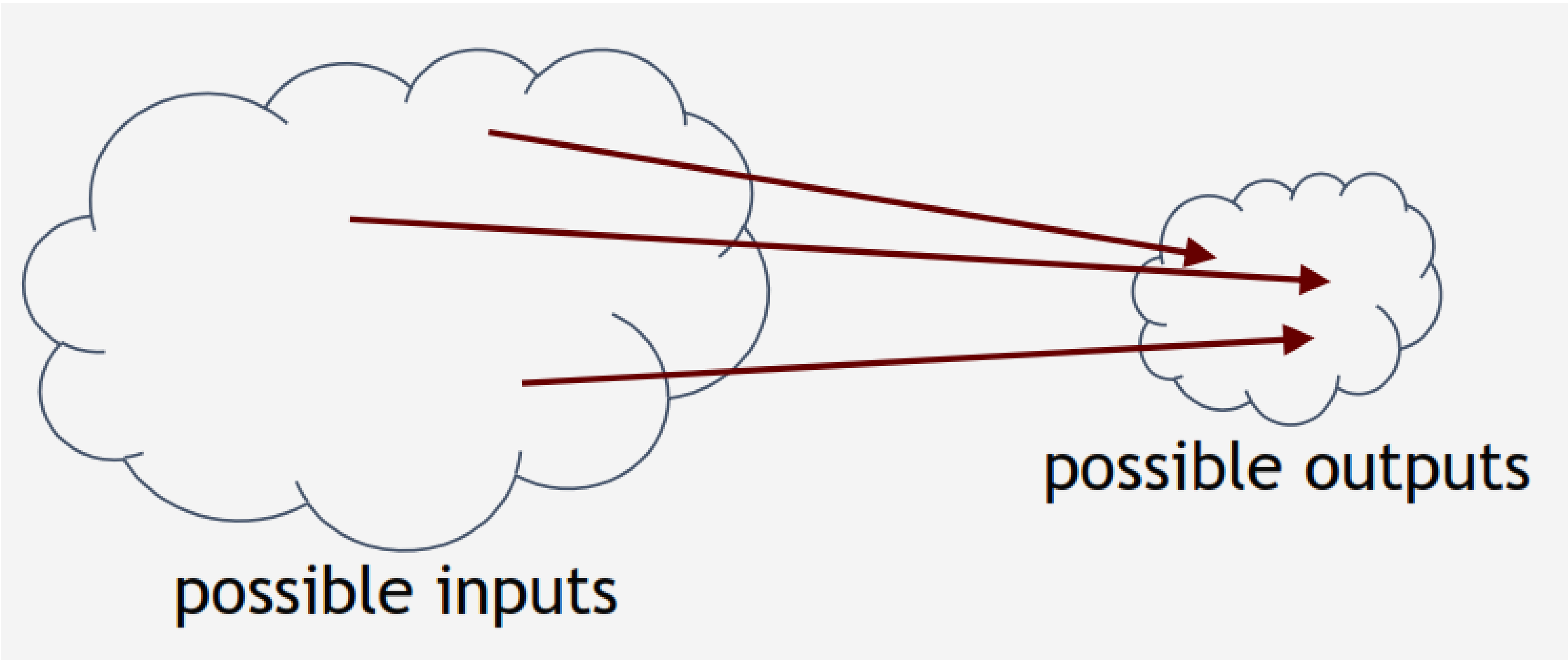
Properties of Message Authentication Codes

1. **Cryptographic checksum** A MAC generates a cryptographically secure authentication tag for a given message.
2. **Symmetric** MACs are based on secret symmetric keys. The signing and verifying parties must share a secret key.
3. **Arbitrary message size** MACs accept messages of arbitrary length.
4. **Fixed output length** MACs generate fixed-size authentication tags.
5. **Message integrity** MACs provide message integrity: Any manipulations of a message during transit will be detected by the receiver.
6. **Message authentication** The receiving party is assured of the origin of the message.
7. **No nonrepudiation** Since MACs are based on symmetric principles, they do not provide nonrepudiation.

Security Properties

- Collision Resistant
- Hiding the original string
- Puzzle Friendly

Collision



How to find Collision

How to find a collision

try 2^{130} randomly chosen inputs
99.8% chance that two of them will collide

This works no matter what H is …
… but it takes too long to matter

- If we know H(x) = H(y),
  - it's safe to assume that x = y.
- To recognize a file that we saw before,
  - just remember its hash.
- Useful because the hash is small.

Is there a faster way to find collisions?
For some possible H's, yes.
For others, we don't know of one.

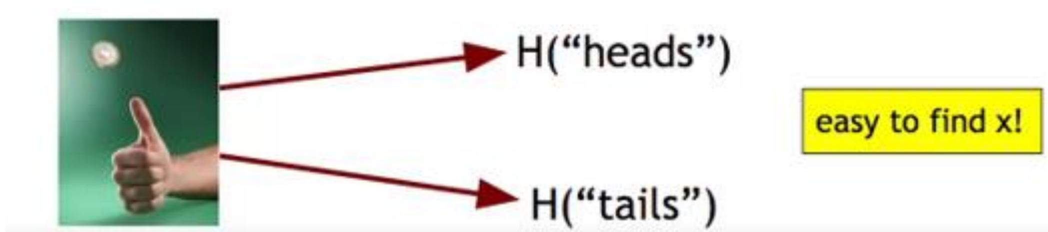
No H has been <u>proven</u> collision-free.

Hiding

Given H(x), it is infeasible to find x.

<u>Hiding property</u>:

- If r is chosen from a probability distribution that has *high min-entropy*, then given H(r | x), it is infeasible to find x.

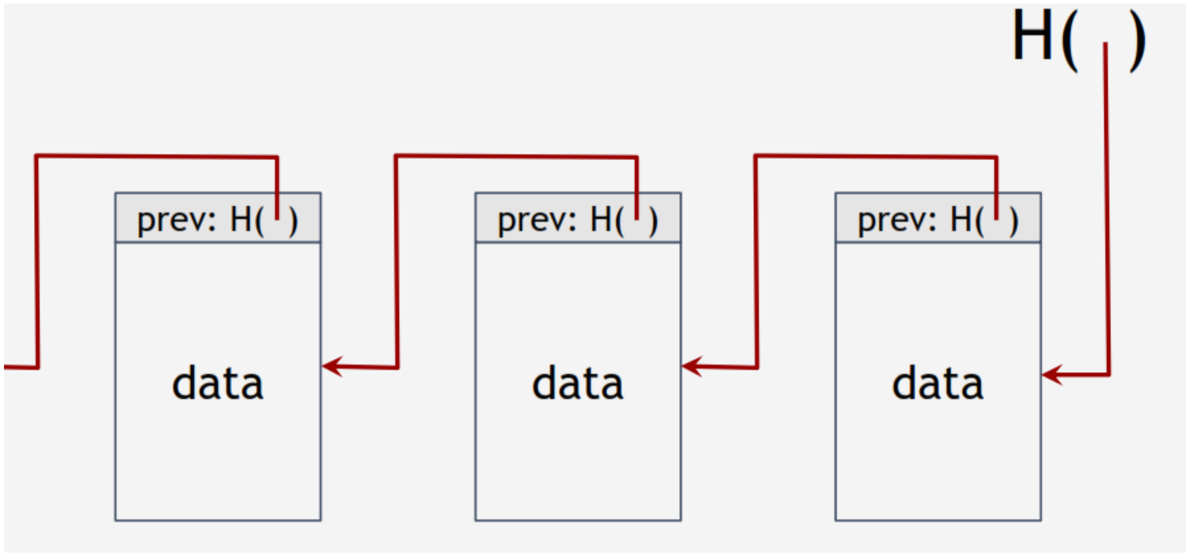


Puzzle Friendly

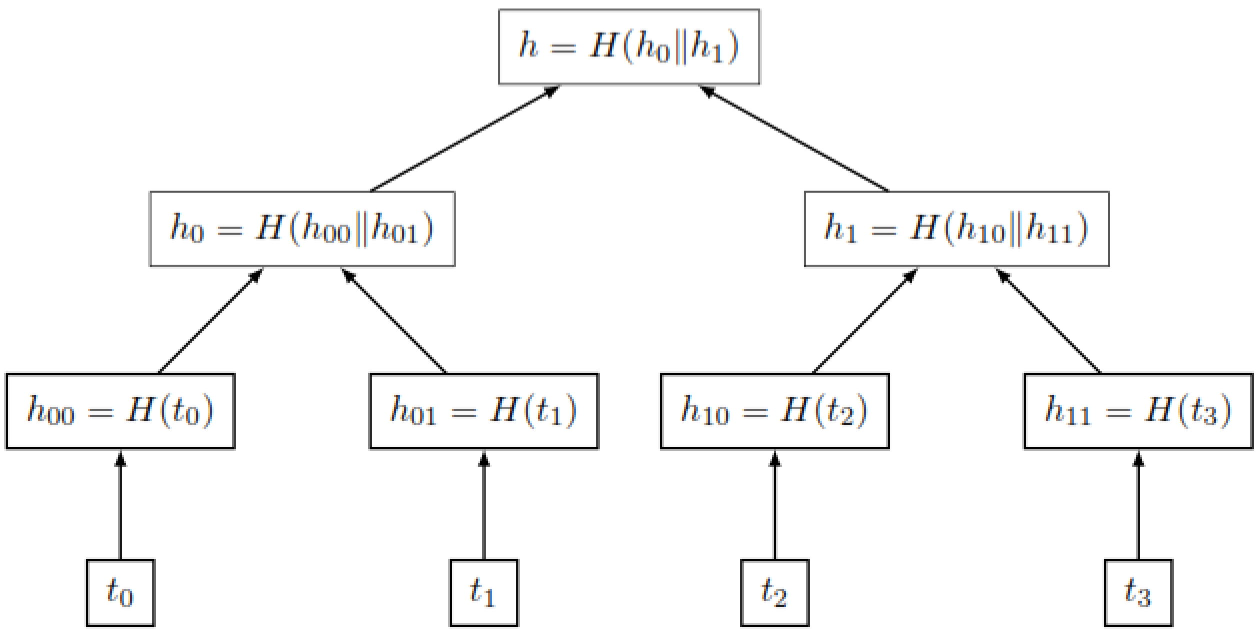
Puzzle-friendly:
For every possible output value y,
if k is chosen from a distribution with high min-entropy,
then it is infeasible to find x such that $H(k \mid x) = y$.

Hash Pointers

- Locate information back
- Verify the integrity

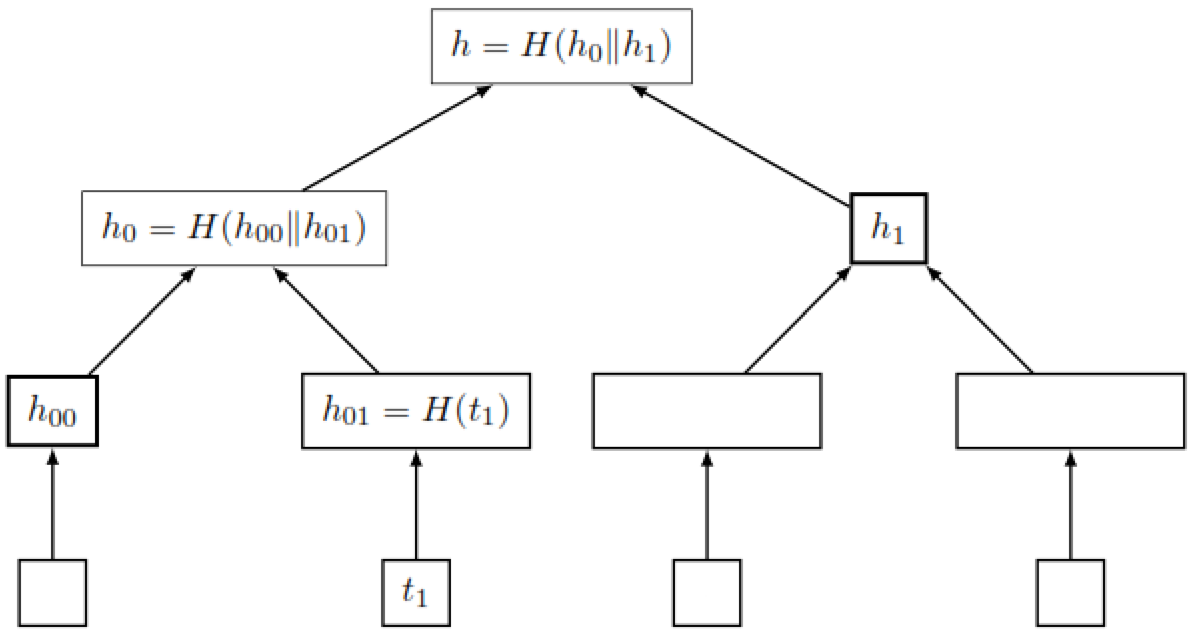


Merkle Tree

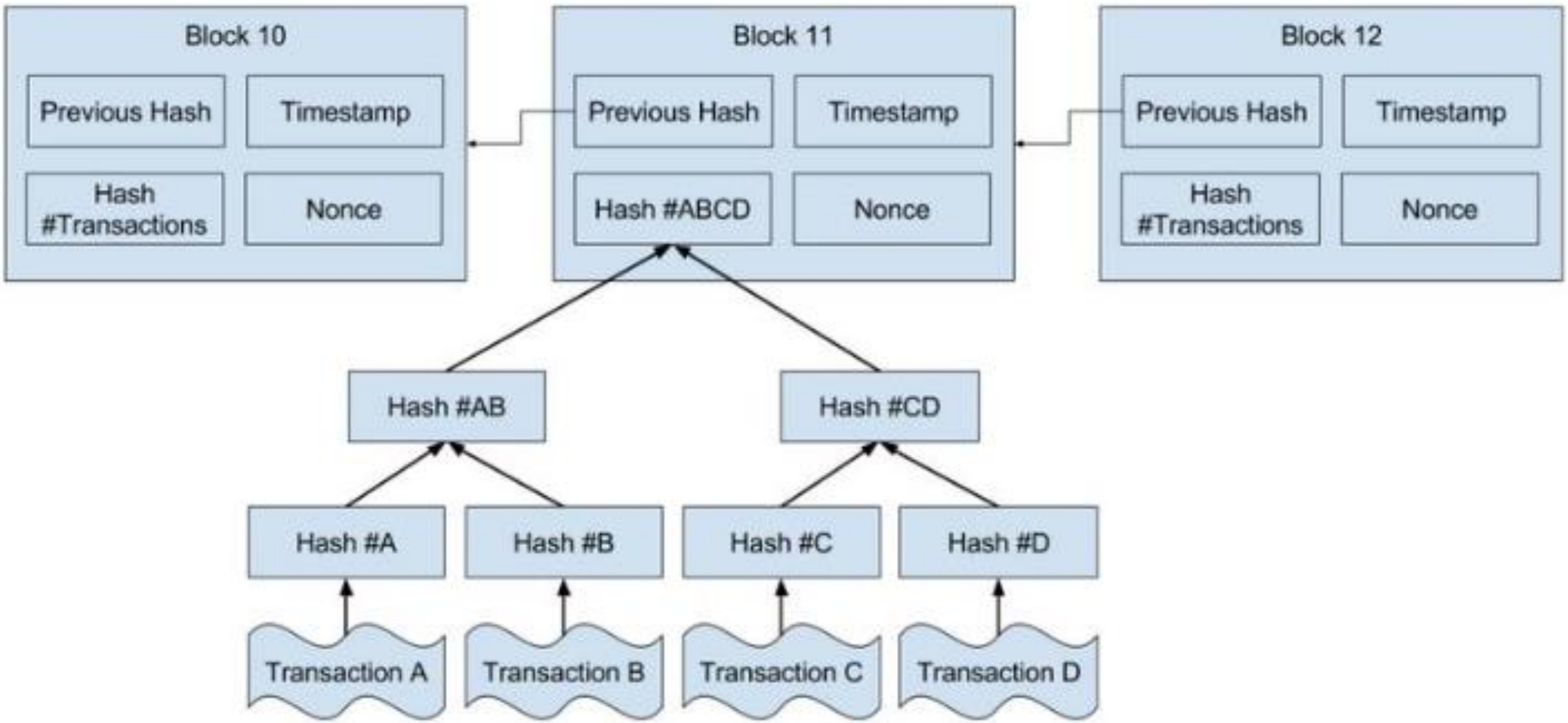


$h = H(h_0 \| h_1)$
$h_0 = H(h_{00} \| h_{01})$
$h_1 = H(h_{10} \| h_{11})$
$h_{00} = H(t_0)$
$h_{01} = H(t_1)$
$h_{10} = H(t_2)$
$h_{11} = H(t_3)$
t_0
t_1
t_2
t_3

To verify O(log n)



Bitcoin



Block 10
Previous Hash
Timestamp
Hash #Transactions
Nonce
Block 11
Previous Hash
Timestamp
Hash #ABCD
Nonce
Block 12
Previous Hash
Timestamp
Hash #Transactions
Nonce
Hash #AB
Hash #CD
Hash #A
Hash #B
Hash #C
Hash #D
Transaction A
Transaction B
Transaction C
Transaction D

Birthday Paradox

- How many people are needed at a party such that there is a reasonable chance that at least two people have the same birthday?

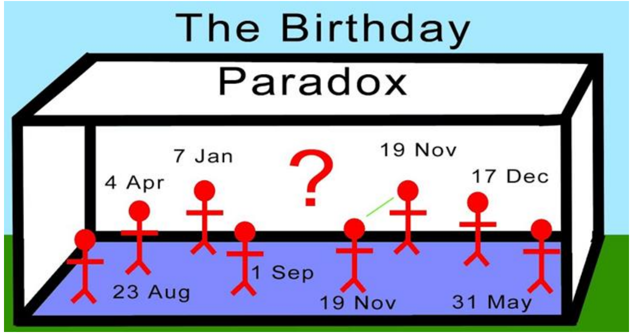
$$P(\text{no collision among 2 people}) = \left(1 - \frac{1}{365}\right)$$

$$P(\text{no collision among 3 people}) = \left(1 - \frac{1}{365}\right) \cdot \left(1 - \frac{2}{365}\right)$$

$$P(\text{no collision among } t \text{ people}) = \left(1 - \frac{1}{365}\right) \cdot \left(1 - \frac{2}{365}\right) \cdots \left(1 - \frac{t-1}{365}\right)$$

$$\begin{aligned} P(\text{at least one collision}) &= 1 - P(\text{no collision}) \\ &= 1 - \left(1 - \frac{1}{365}\right) \cdots \left(1 - \frac{23-1}{365}\right) \\ &= 0.507 \approx 50\%. \end{aligned}$$

[40 with 90%
Hashing with 2^n
it is sqrt (2^n)



Birthday Paradox

What is the probability that two people have the same birthday (day and month)

K	Total	Different
2	365^2	365×364
3	365^3	$365 \times 364 \times 363$
	$\cdots$	
k	365^k	$365 \times 364 \times 363 \times \cdots \times (365 - k + 1)$

$$P(\text{No common day}) = \frac{365 \times 364 \times 363 \times \ldots \times (365 - k + 1)}{365^k}$$

K

$$= \frac{365!}{365^k (365 - k)!}$$

k	P
2	.01
3	.02
4	.03
...	...
19	.41
20	.44
21	.48
22	.51
23	.54
...	...
38	.88
39	.89
40	.90

ECC over fields

Example 9.1. Let's look at the polynomial equation $x^2 + y^2 = r^2$ over the real numbers $\mathbb{R}$. If we plot all the pairs (x, y) which fulfill this equation in a coordinate sys-

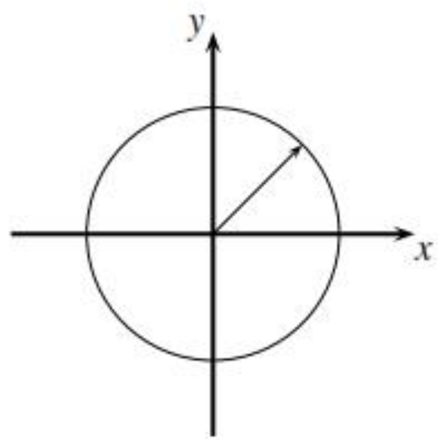


Fig. 9.1 Plot of all points (x, y) which fulfill the equation $x^2 + y^2 = r^2$ over $\mathbb{R}$

tem, we obtain a circle as shown in Fig. 9.1.

◇

ECC

Example 9.2. A slight generalization of the circle equation is to introduce coefficients to the two terms x^2 and y^2, i.e., we look at the set of solutions to the equation $a \cdot x^2 + b \cdot y^2 = c$ over the real numbers. It turns out that we obtain an ellipse, as

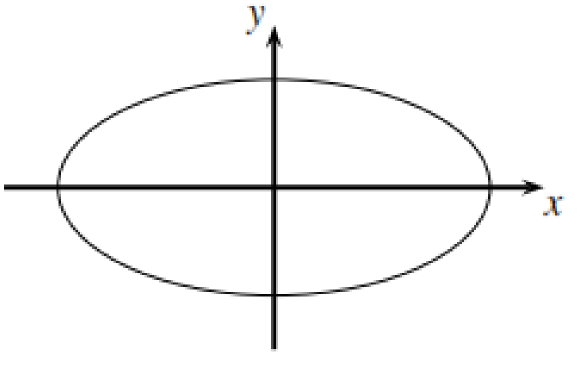


Fig. 9.2 Plot of all points (x, y) which fulfill the equation $a \cdot x^2 + b \cdot y^2 = c$ over $\mathbb{R}$

ECC Definition

- An elliptic curve is a special type of polynomial equation

The elliptic curve *over* $\mathbb{Z}_p$, $p > 3$, *is the set of all pairs* $(x, y) \in \mathbb{Z}_p$ *which fulfill*

$$y^2 \equiv x^3 + a \cdot x + b \bmod p \qquad (9.1)$$

together with an imaginary point of infinity $\mathcal{O}$, *where*

$$a, b \in \mathbb{Z}_p$$

and the condition $4 \cdot a^3 + 27 \cdot b^2 \neq 0 \bmod p$.

ECC

Example 9.3. In Figure 9.3 the elliptic curve $y^2 = x^3 - 3x + 3$ is shown over the real numbers.

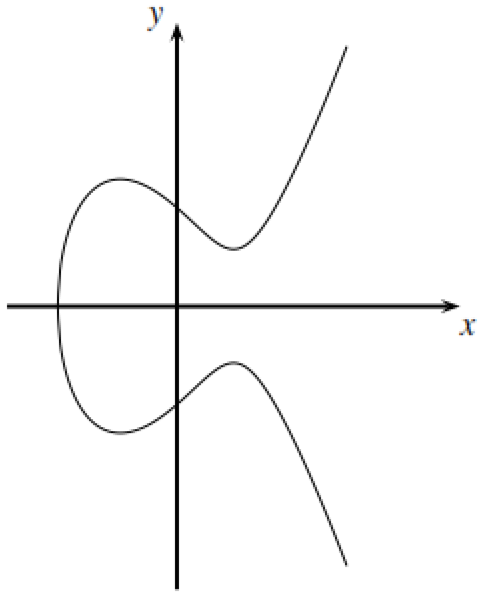


Fig. 9.3 $y^2 = x^3 - 3x + 3$ over $\mathbb{R}$

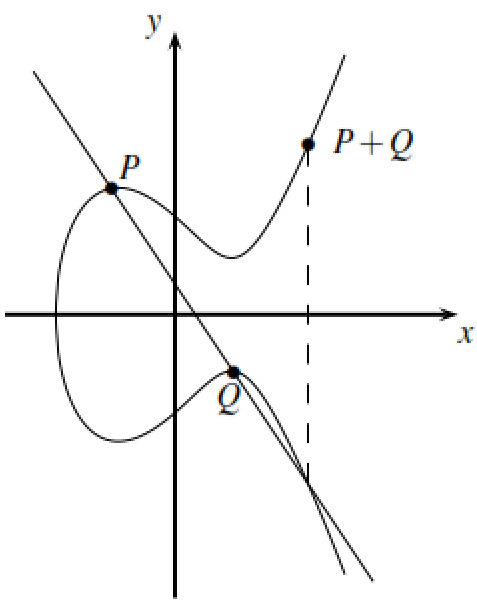
ECC operations

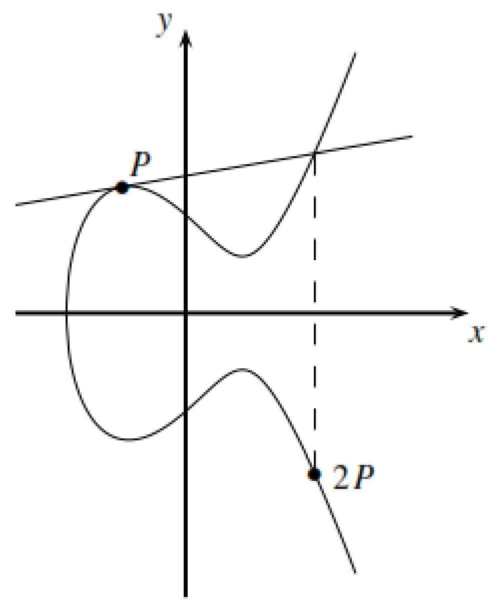
Let's denote the group operation with the addition symbol[2] "+". "Addition" means that given two points and their coordinates, say $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, we have to compute the coordinates of a third point R such that:

$$P + Q = R$$

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

Point addition / Doubling





Elliptic Curve Point Addition and Point Doubling

$$
\begin{aligned}
x_3 &= s^2 - x_1 - x_2 \bmod p \\
y_3 &= s(x_1 - x_3) - y_1 \bmod p
\end{aligned}
$$

where

$$
s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p \text{ ; if } P \neq Q \text{ (point addition)} \\ \frac{3x_1^2 + a}{2y_1} \bmod p \text{ ; if } P = Q \text{ (point doubling)} \end{cases}
$$

$$P + \mathcal{O} = P$$

$$P + (-P) = \mathcal{O}.$$

$$-P = (x_p, p - y_p).$$

Illustration

$$E : y^2 \equiv x^3 + 2x + 2 \bmod 17.$$

We want to double the point $P = (5,1)$.

$$\begin{aligned}
2P &= P + P = (5,1) + (5,1) = (x_3, y_3) \\
s &= \frac{3x_1^2 + a}{2y_1} = (2 \cdot 1)^{-1}(3 \cdot 5^2 + 2) = 2^{-1} \cdot 9 \equiv 9 \cdot 9 \equiv 13 \bmod 17 \\
x_3 &= s^2 - x_1 - x_2 = 13^2 - 5 - 5 = 159 \equiv 6 \bmod 17 \\
y_3 &= s(x_1 - x_3) - y_1 = 13(5-6) - 1 = -14 \equiv 3 \bmod 17 \\
2P &= (5,1) + (5,1) = (6,3)
\end{aligned}$$

$$\begin{aligned}
y^2 &\equiv x^3 + 2 \cdot x + 2 \bmod 17 \\
3^2 &\equiv 6^3 + 2 \cdot 6 + 2 \bmod 17 \\
9 &= 230 \equiv 9 \bmod 17
\end{aligned}$$

Illustration

$$
\begin{aligned}
2P &= (5,1)+(5,1)=(6,3) \\
3P &= 2P+P=(10,6) \\
4P &= (3,1) \\
5P &= (9,16) \\
6P &= (16,13) \\
7P &= (0,6) \\
8P &= (13,7) \\
9P &= (7,6) \\
10P &= (7,11)
\end{aligned}
$$

$$
\begin{aligned}
11P &= (13,10) \\
12P &= (0,11) \\
13P &= (16,4) \\
14P &= (9,1) \\
15P &= (3,16) \\
16P &= (10,11) \\
17P &= (6,14) \\
18P &= (5,16) \\
19P &= \mathcal{O}
\end{aligned}
$$

From now on, the cyclic structure becomes visible since:

$$
\begin{aligned}
20P &= 19P+P=\mathcal{O}+P=P \\
21P &= 2P
\end{aligned}
$$

Definition 9.2.1 Elliptic Curved Discrete Logarithm Problem (ECDLP)

Given is an elliptic curve E. We consider a primitive element P and another element T. The DL problem is finding the integer d, where $1 \leq d \leq \#E$, such that:

$$\underbrace{P+P+\cdots+P}_{d \;\; times} = dP = T. \tag{9.2}$$

ECC Encryption

- Several approaches using elliptic curves have been analyzed
- Must first encode any message *m* as a point on the elliptic curve P_m
- Select suitable curve and point G as in Diffie-Hellman
- Each user chooses a private key n_A and generates a public key $P_A = n_A * G$
- To encrypt and send message P_m to B, A chooses a random positive integer *k* and produces the ciphertext C_m *consisting of the pair of points:*

$$C_m = \{kG, P_m + kP_B\}$$

- To decrypt the ciphertext, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point:

$$P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m$$

ECDH

ECDH Domain Parameters

1. Choose a prime p and the elliptic curve

$$E : y^2 \equiv x^3 + a \cdot x + b \bmod p$$

2. Choose a primitive element $P = (x_P, y_P)$

The prime p, the curve given by its coefficients a, b, and the primitive element P are the domain parameters.

Elliptic Curve Diffie–Hellman Key Exchange (ECDH)

Alice		**Bob**
choose $k_{prA} = a \in \{2, 3, \ldots, \#E-1\}$		choose $k_{prB} = b \in \{2, 3, \ldots, \#E-1\}$
compute $k_{pubA} = aP = A = (x_A, y_A)$		compute $k_{pubB} = bP = B = (x_B, y_B)$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
compute $aB = T_{AB}$		compute $bA = T_{AB}$

Joint secret between Alice and Bob: $T_{AB} = (x_{AB}, y_{AB})$.

Bitcoin Address

$$y^2 = (x^3 + 7) \text{ over } (\mathbb{F}_p)$$

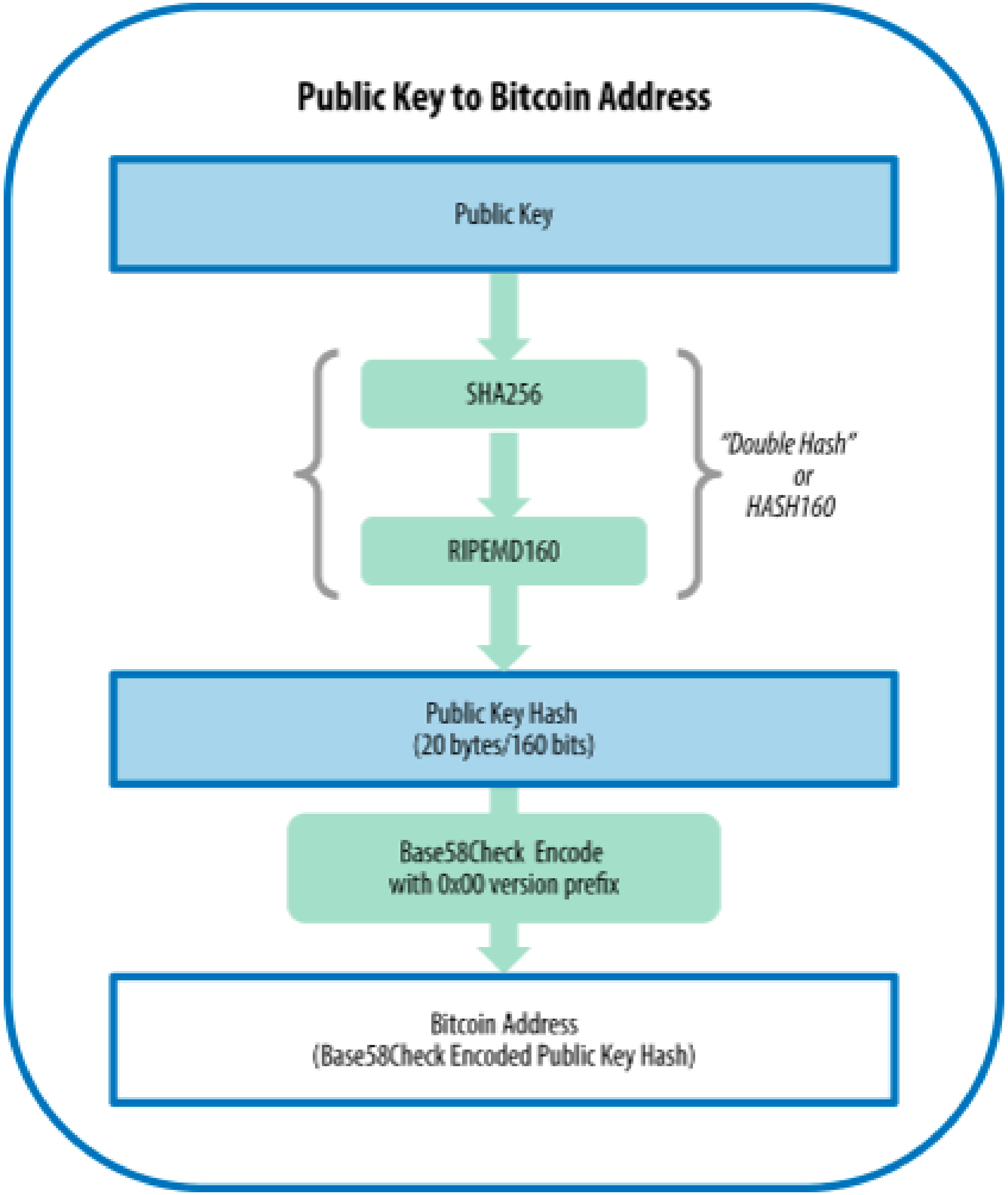
or

$$y^2 \bmod p = (x^3 + 7) \bmod p$$

```
$ bitcoind getnewaddress
1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy
$ bitcoind dumpprivkey 1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy
KxFC1jmwwCoACiCAWZ3eXa96mBM6tb3TYzGmf6YwgdGWZgawvrtJ
```

$$A = RIPEMD160(SHA256(K))$$

where K is the public key and A is the resulting bitcoin address.


Public Key to Bitcoin Address
Public Key
SHA256
RIPEMD160
"Double Hash"
or
HASH160
Public Key Hash
(20 bytes/160 bits)
Base58Check Encode
with 0x00 version prefix
Bitcoin Address
(Base58Check Encoded Public Key Hash)

Bitcoin addresses

- 2^160 addresses

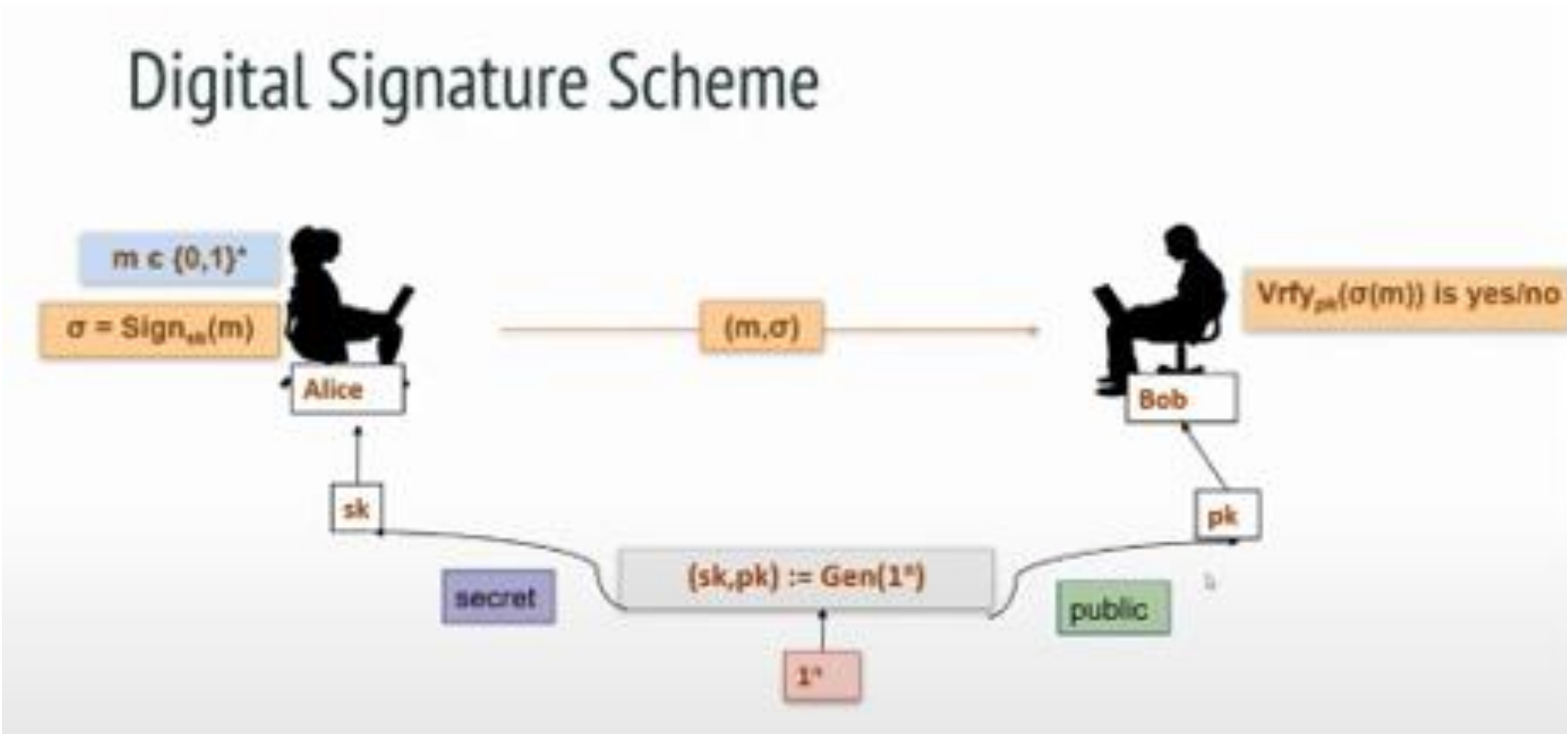
1.46 × 10^48 possible
Bitcoin Addresses

2.05×10^38 Different
Addresses

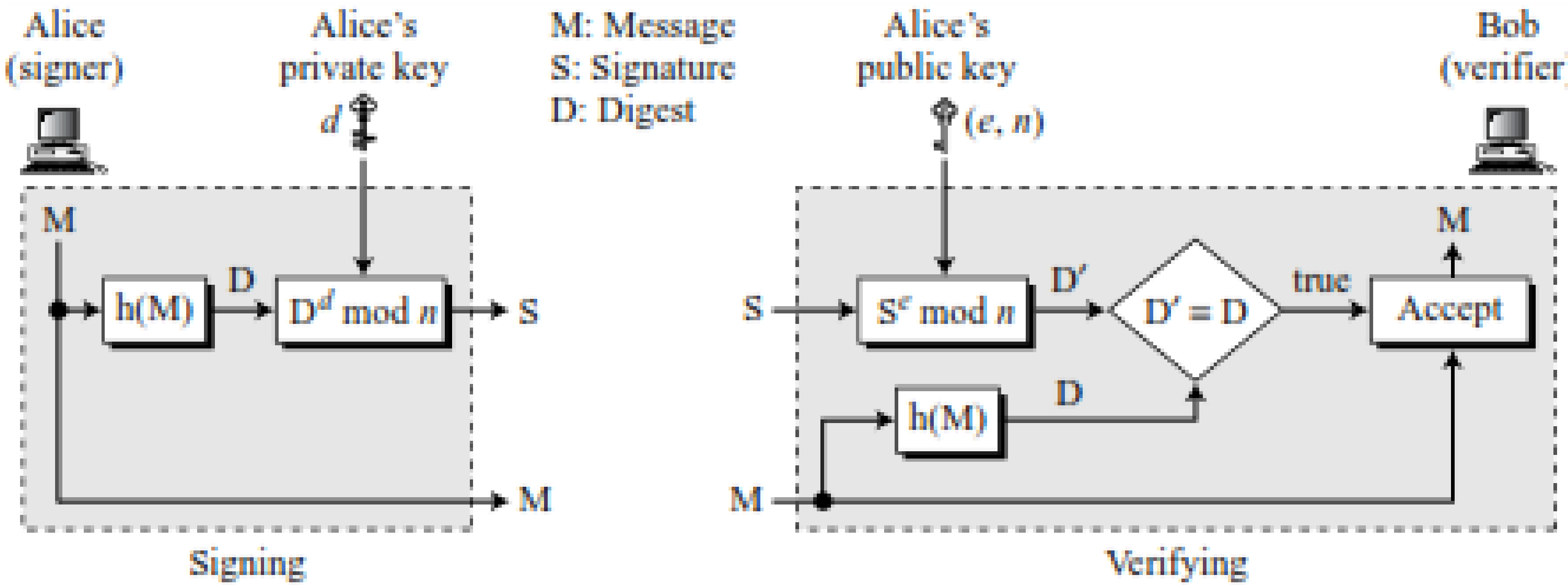
Digital Signature

- Operation is similar to that of the MAC
- The hash value of a message is encrypted with a user's private key
- Anyone who knows the user's public key can verify the integrity of the message
- An attacker who wishes to alter the message would need to know the user's private key
- Implications of digital signatures go beyond just message authentication

Digital Signature



RSA Digital Signature



ECC

- Satoshi chose the parameters of the standard secp256k1 for Bitcoin
- Y^2=x^3+ax+b mod P
- Bitcoin
- Y^2 = x^3+7 mod p

Bitcoin Block Rewards

Block 000000 to 209999, total reward = 50

Block 210000 to 419999 total reward = 25

Block 420000 to 629999 total reward = 12.5

Block 630000 to 839999 total reward = 6.25

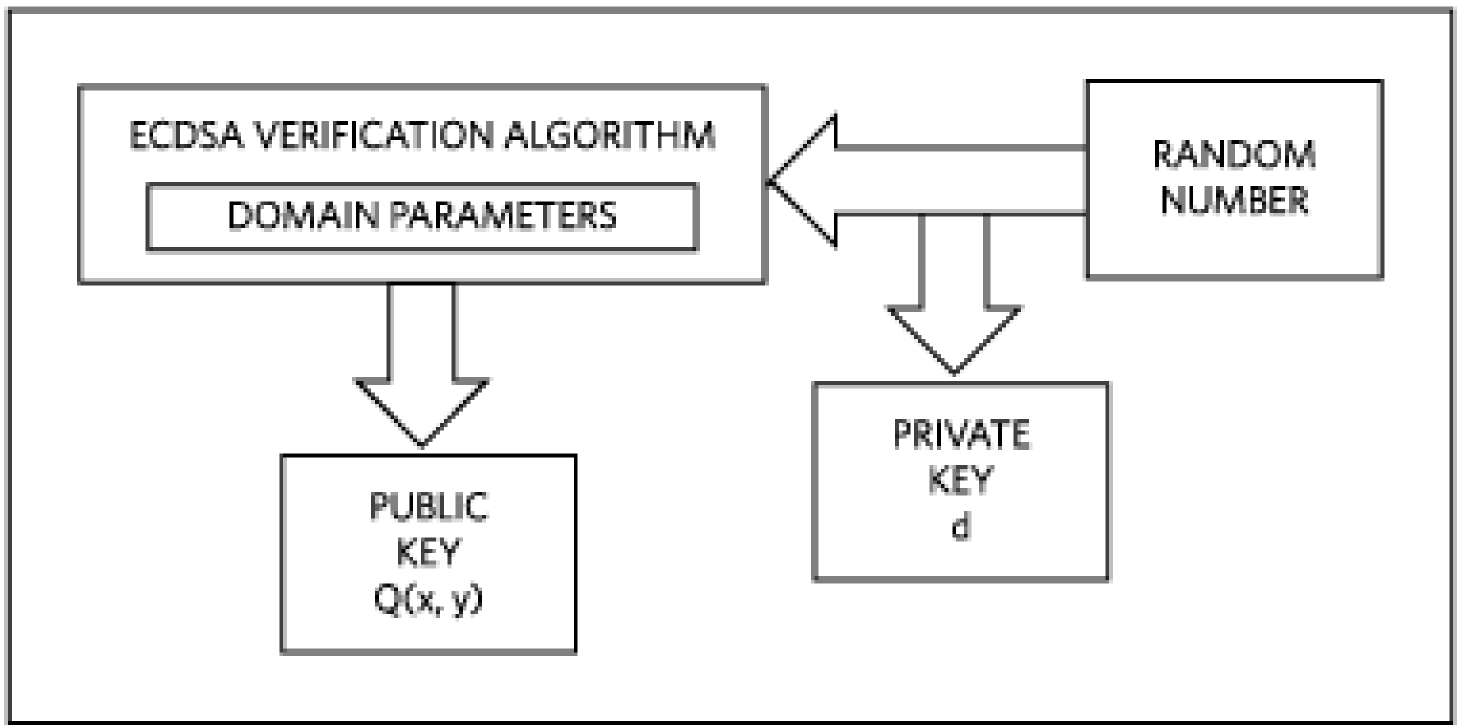
Openssl Commands

- openssl ecparam -name prime256v1 -genkey -noout -out eckey.pem
- gedit eckey.pem
- openssl ec -inform pem -in eckey.pem –pubout >eckey.pub
- openssl ecparam -name prime256v1 -genkey -noout -out alice_privkey.pem
- openssl ec -inform pem -in alice_privkey.pem -pubout >alice_pubkey.pem
- gedit alice_pubkey.pem
- gedit alice_privkey.pem
- openssl ecparam -name prime256v1 -genkey -noout -out bob_privkey.pem
- openssl ec -inform pem -in bob_privkey.pem -pubout >bob_pubkey.pem

Finite Field

- Bitcoin uses Finite field arithmetic
- IEEE 2019, error in rounding
- 0.1+0.2 = 0.30000000000000004

ECDSA


ECDSA VERIFICATION ALGORITHM
DOMAIN PARAMETERS
RANDOM NUMBER
PUBLIC KEY Q(x, y)
PRIVATE KEY d

Key Generation

Key Generation for ECDSA

1. Use an elliptic curve E with
   - modulus p
   - coefficients a and b
   - a point A which generates a cyclic group of prime order q
2. Choose a random integer d with $0 < d < q$.
3. Compute $B = d\,A$.

The keys are now:

$k_{pub} = (p, a, b, q, A, B)$

$k_{pr} = (d)$

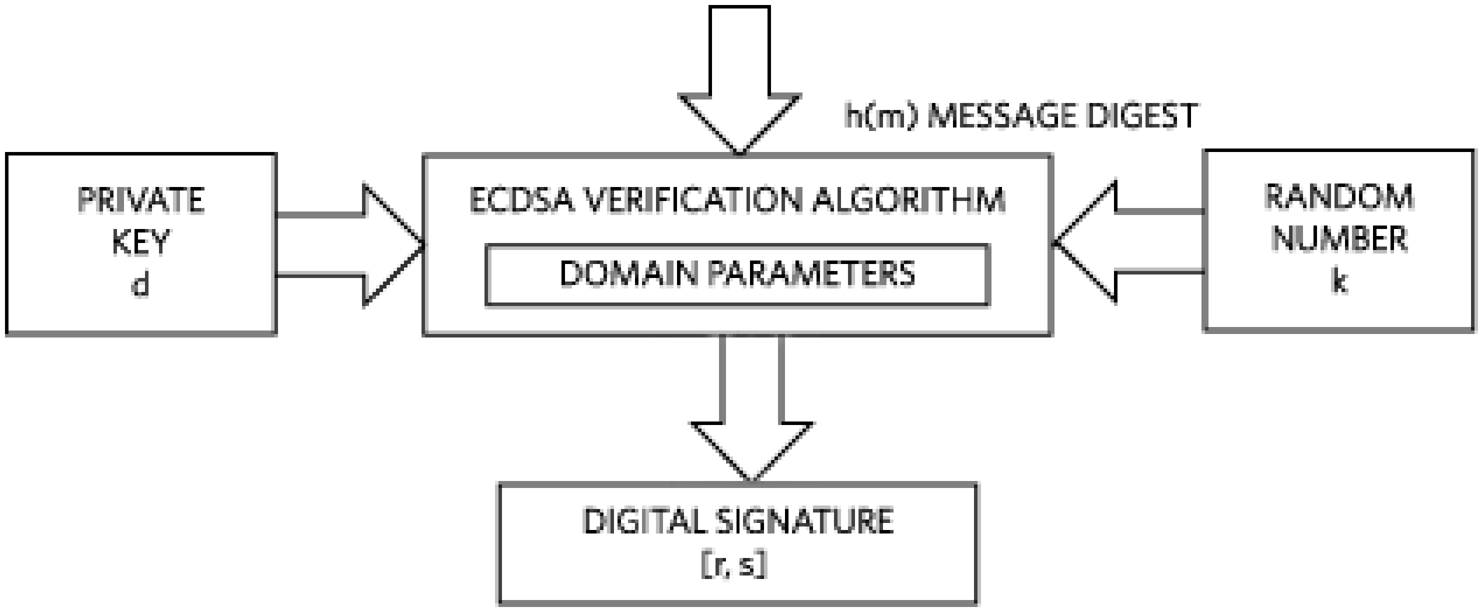
Signature Generation

- (r,s) fairly short signatures

ECDSA Signature Generation

1. Choose an integer as random ephemeral key k_E with $0 < k_E < q$.
2. Compute $R = k_E A$.
3. Let $r = x_R$.
4. Compute $s \equiv (h(x) + d \cdot r)\, k_E^{-1} \bmod q$.

Signature Generation



Verification

ECDSA Signature Verification

1. Compute auxiliary value $w \equiv s^{-1} \bmod q$.
2. Compute auxiliary value $u_1 \equiv w \cdot h(x) \bmod q$.
3. Compute auxiliary value $u_2 \equiv w \cdot r \bmod q$.
4. Compute $P = u_1 A + u_2 B$.
5. The verification $ver_{k_{pub}}(x, (r, s))$ follows from:

$$x_P \begin{cases} \equiv r \bmod q \Longrightarrow \text{valid signature} \\ \not\equiv r \bmod q \Longrightarrow \text{invalid signature} \end{cases}$$

Illustration

$$E : y^2 \equiv x^3 + 2x + 2 \bmod 17$$

sign:
compute hash of message $h(x) = 26$
choose ephemeral key $k_E = 10$
$R = 10 \cdot (5,1) = (7,11)$
$r = x_R = 7$
$s = (26 + 7 \cdot 7) \cdot 2 \equiv 17 \bmod 19$

Bob
choose E with $p = 17$, $a = 2$, $b = 2$, and
$A = (5,1)$ with $q = 19$
choose $d = 7$
compute $B = dA = 7 \cdot (5,1) = (0,6)$

verify:
$w = 17^{-1} \equiv 9 \bmod 19$
$u_1 = 9 \cdot 26 \equiv 6 \bmod 19$
$u_2 = 9 \cdot 7 \equiv 6 \bmod 19$
$P = 6 \cdot (5,1) + 6 \cdot (0,6) = (7,11)$
$x_P \equiv r \bmod 19 \Longrightarrow$ valid signature

Identities

- Public key has identity
- Pk identity
- Sk speaks for the identity

Pseudo Anonymity

- https://www.technologyreview.com/2017/08/23/149531/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/

Demo

- https://andersbrownworth.com/blockchain/blockchain
- Anyhash.com
- https://andersbrownworth.com/blockchain/public-private-keys/keys
- https://prathamudeshmukh.github.io/merkle-tree-demo/

Bitcoin Blockchain

- Bitcoin Blockchain Size
- 451.34 GB for Jan 31 2023

Thank You