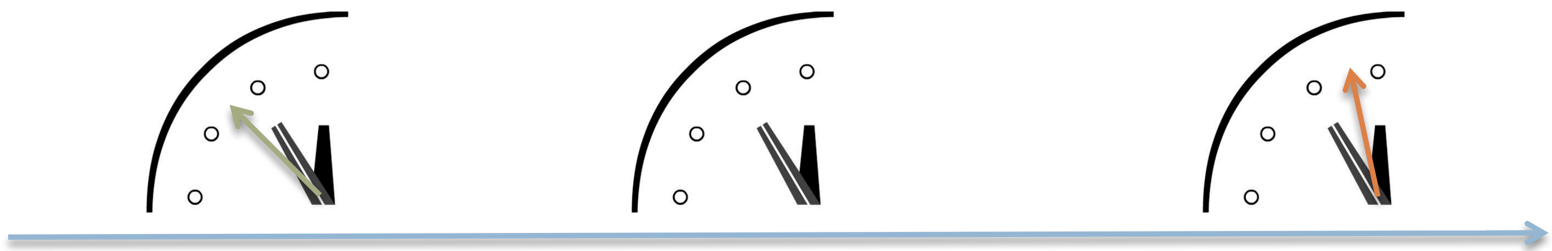
SECRET SHARING SCHEMES

Kristin Stenerson and Mark Ibrahim

A Critical Moment



1947

1949

1953

7 MINUTES TO MIDNIGHT
Clock appears for the first time to communicate the threat nuclear weapons pose

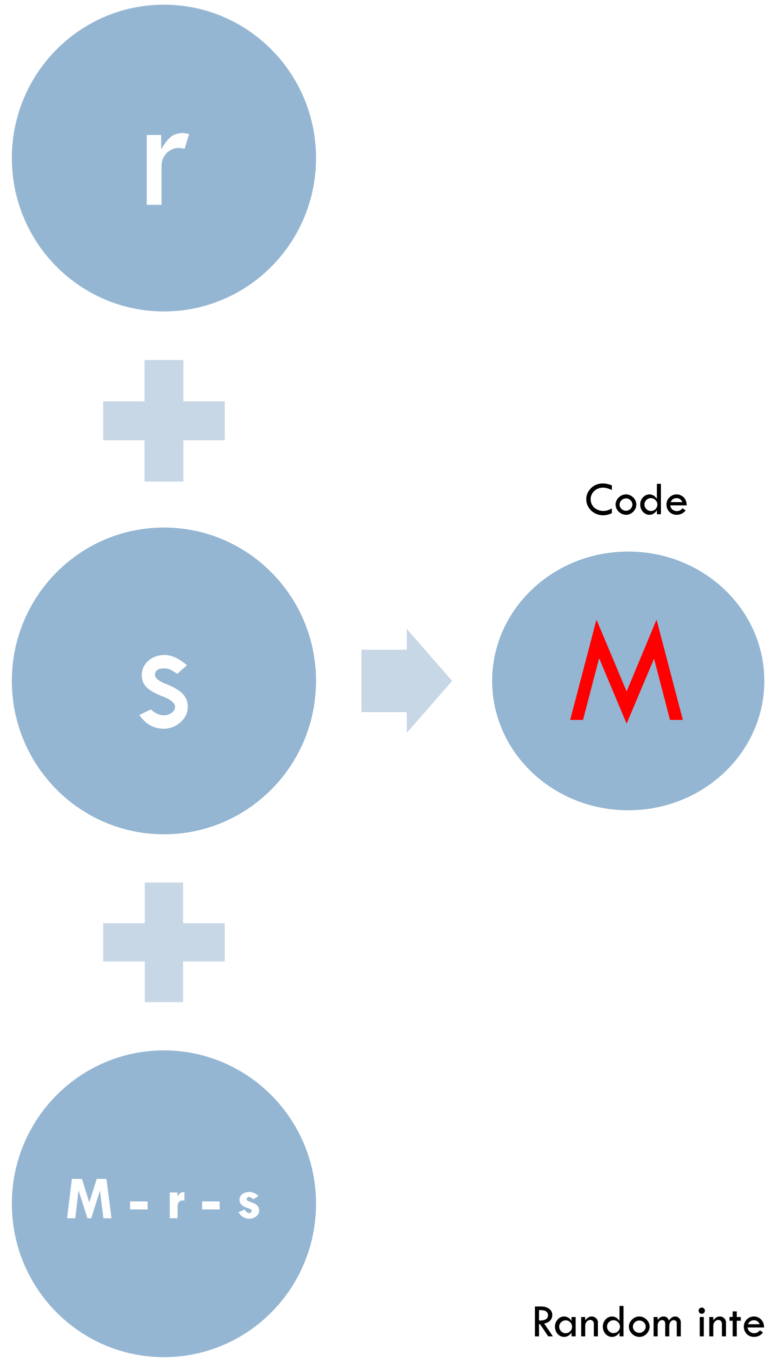
3 MINUTES TO MIDNIGHT
1949: President Harry Truman tells the American public that the Soviets tested their first nuclear device, officially starting the arms race.

2 MINUTES TO MIDNIGHT
1953: United States tests its first thermonuclear device; the Soviets test an H-bomb of their own.

President, Dwight Eisenhower:

VP, Richard Nixon:

NSA, John Ackerman:

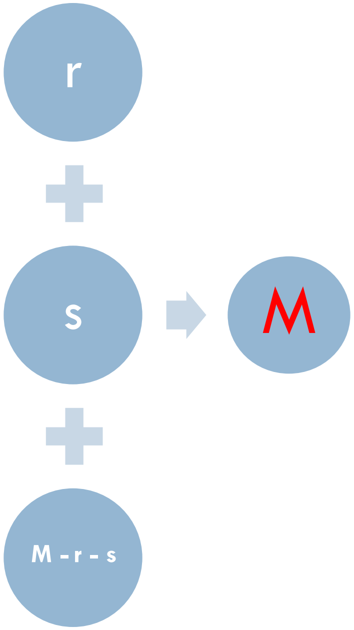


Random integers: r, s

Practical Limits: working mod n

Random number generation

- Computers difficulty quickly processing computations for large numbers
- Work mod n for some n larger than the code M:



(mod n)

- Sufficiently large n will not interfere with calculations

Why can't we try all possible values of r and s (mod n)?

- Finite set of possible passwords mod n:

$$\{0,1,2,3,\ldots,n-1\}$$

- Random integers: r (mod n) and s (mod n)

- Modern computing limits brute force approaches:

Fastest computer *Tihani-1A* computes:

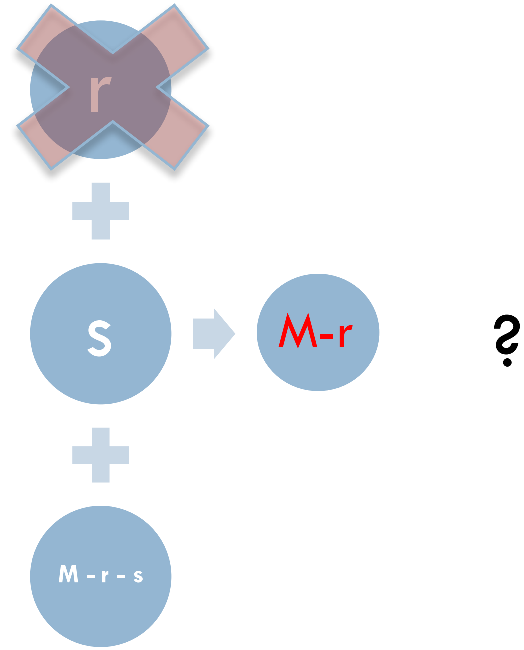
2.5*10^15 mathematical operations per sec

$n = 10^{12} \longrightarrow 10^{12} \times 10^{12} = 10^{24}$

750 years!

What if Russians guess the president is on the committee and assassinate him?

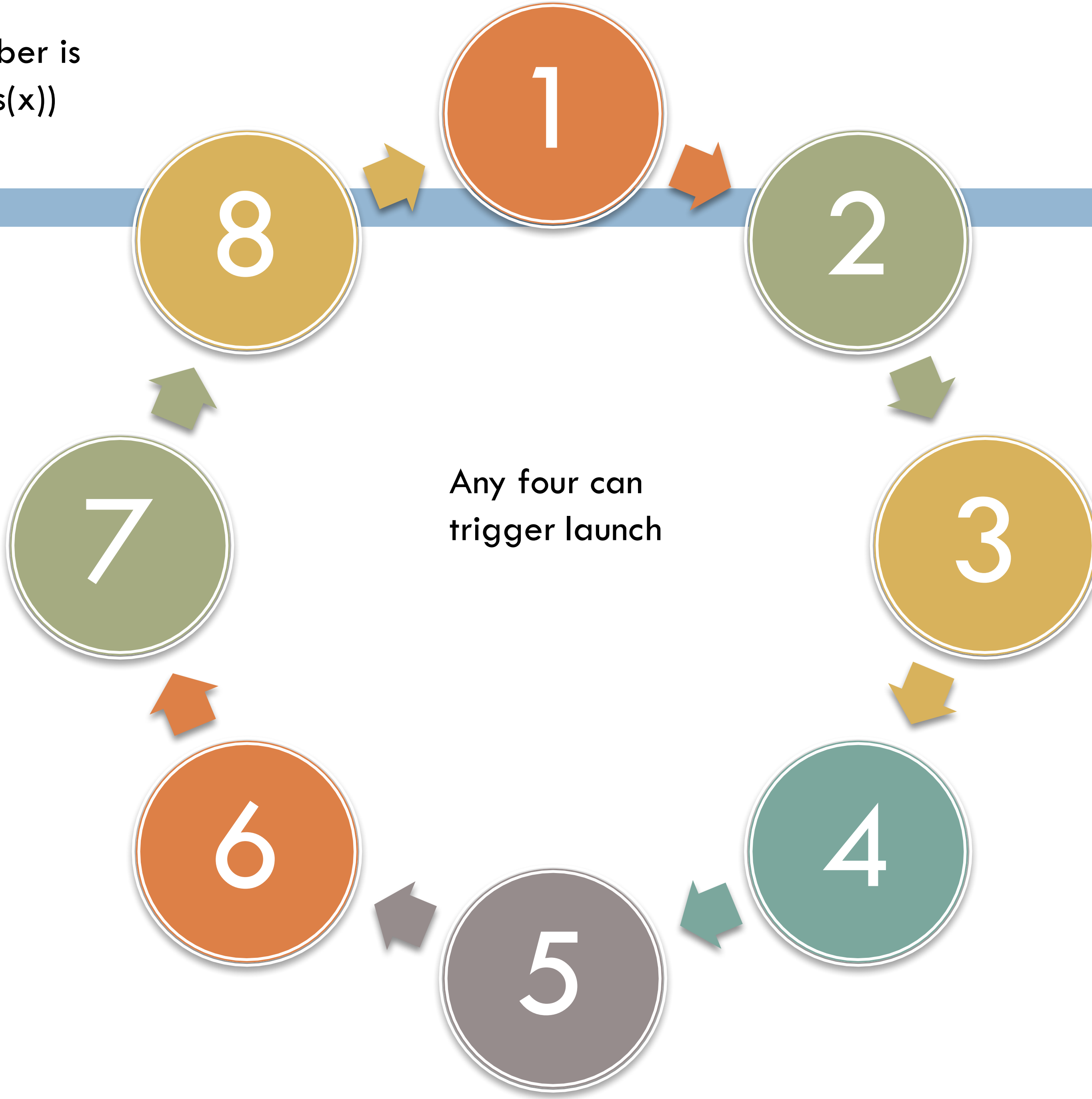
M – r – s (mod n):



The whole country is compromised !

- A scheme requiring only a subset of the members on the committee is needed…

Each member is given: (x, s(x))



Any four can trigger launch

A Better Method to Share a Secret

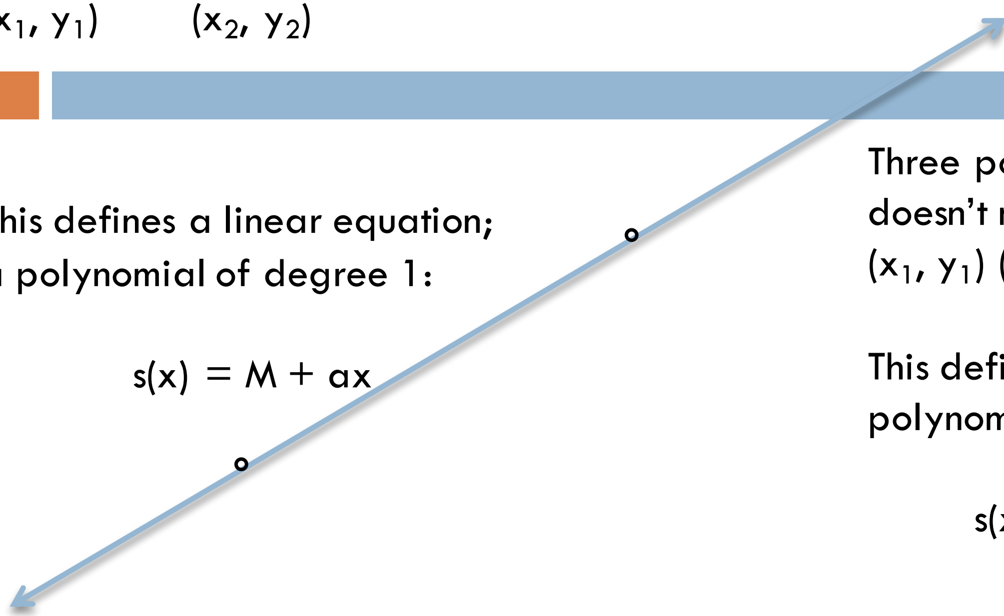
- Secret: M (a number)
- We want to split M between 8 people
- Prime: p (any prime > M)
- Construct a polynomial:

$$S(x) = M + s_1 x + s_2 x^2 + s_3 x^3 \ (mod\ p)$$

- Distribute 8 pairs (x_i, y_i) where $y_i = S(x_i)$
- Any subset of 4 pairs can determine the secret

Two points define a line;
doesn't matter which two:

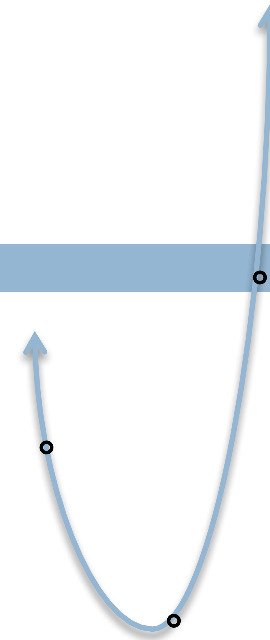
(x_1, y_1) (x_2, y_2)



This defines a linear equation;
a polynomial of degree 1:

$$s(x) = M + ax$$

Three points define a quadratic;
doesn't matter which three:
(x_1, y_1) (x_2, y_2) (x_3, y_3)



This defines a linear equation; a polynomial of degree 2:

$$s(x) = M + a_1 x + a_2 x^2$$

Any set of t points, define a polynomial of degree t-1:

$$\boxed{s(x) = M + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1}}$$

e.g., 4 to activate launch so we need to define a polynomial of degree 3

If we can generate any polynomial that passes through 4 points on $s(x)$, then it MUST be $s(x)$

(4,8)- Threshold Scheme
Secret Launch Code

Secret: "WIN"

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

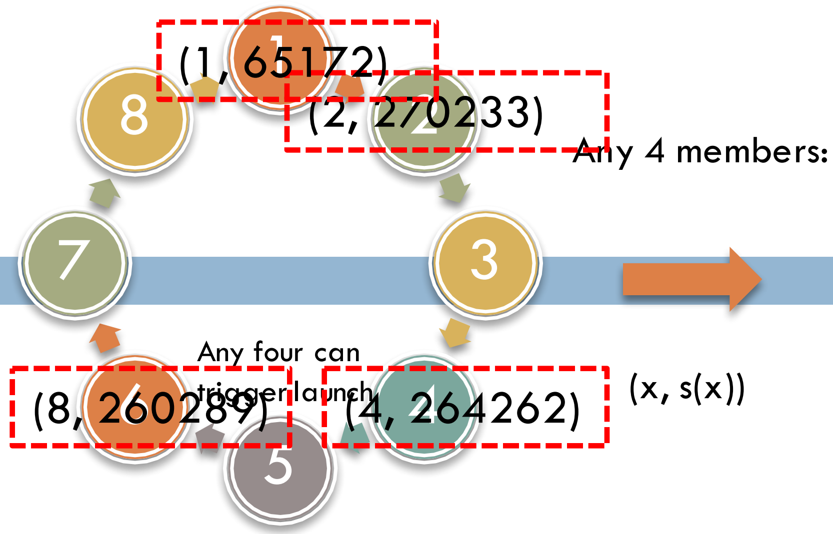
W -> 22

I -> 08

N -> 13

So our secret is 220813

Prime p=319,993



- Generate:

$$s(x) = M + ax + bx^2 + cx^3 \pmod{319993}$$

$$M \quad a \quad b \quad c \rightarrow s(x)$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \\ 1 & 4 & 16 & 64 \\ 1 & 8 & 64 & 512 \end{bmatrix} \begin{bmatrix} M \\ a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 65172 \\ 270233 \\ 264262 \\ 260289 \end{bmatrix} \longrightarrow \begin{bmatrix} M \\ a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 220813 \\ 152478 \\ 87632 \\ 244235 \end{bmatrix}$$

- $S(x) = 220813 + 152478x + 87632x^2 + 244235x^3 \ (mod\ 319993)$
- M = 220813

Country is safe!

Newton Interpolant

- Reconstruct $S(x)$ using a nonstandard basis:

$$\{1, x - x_1, (x - x_1)(x - x_2), (x - x_1)(x - x_2)(x - x_3)\}$$

- Create:

$$P(x) = c_0 + c_1(x - x_1) + c_2(x - x_1)(x - x_2) + c_3(x - x_1)(x - x_2)(x - x_3)$$

- Form the following system of equations

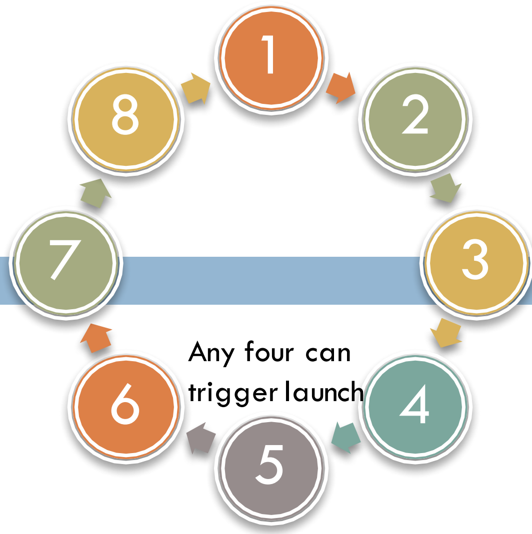
$$P(x_1) = c_0 = y_1$$
$$P(x_2) = c_0 + c_1(x_2 - x_1) = y_2$$
$$P(x_3) = c_0 + c_1(x_3 - x_1) + c_2(x_3 - x_1)(x_3 - x_2) = y_3$$
$$P(x_4) = c_0 + c_1(x_4 - x_1) + c_2(x_4 - x_1)(x_4 - x_2) + c_3(x_4 - x_1)(x_4 - x_2)(x_4 - x_3) = y_4$$

The Newton Trick

- Solve the system for the c_i's to get $S(x)$
- Form a Matrix Equation

$$\begin{bmatrix} \boxed{1} & 0 & 0 & 0 \\ 1 & \boxed{(x_2 - x_1)} & 0 & 0 \\ 1 & (x_3 - x_1) & \boxed{(x_3 - x_1)(x_3 - x_2)} & 0 \\ 1 & (x_4 - x_1) & (x_4 - x_1)(x_4 - x_2) & \boxed{(x_4 - x_1)(x_4 - x_2)(x_4 - x_3)} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix}$$

- Our matrix is lower triangular
  - Determinant is product of main diagonal entries $\neq 0$
  - Thus, the system has a unique solution
  - Because of the basis we chose, we can solve for the c_i's by back substitution, no matrix operations are necessary



Any 4 members:

(4, 264262)

(1, 65172)

(x, s(x))

(2, 270233)

(8, 260289)

- Form the Polynomial:

$$P(x) = c_0 + c_1(x - x_1) + c_2(x - x_1)(x - x_2) + c_3(x - x_1)(x - x_2)(x - x_3)$$

$$P(x) = c_0 + c_1(x - 1) + c_2(x - 1)(x - 2) + c_3(x - 1)(x - 2)(x - 4)$$

- Form the System of Equations:

$$P(1) = c_0 = 65172$$

$$P(2) = c_0 + c_1 = 270233$$

$$P(4) = c_0 + 3c_1 + 6c_2 = 264262$$

$$P(8) = c_0 + 7c_1 + 42c_2 + 168c_3 = 260289$$

Newton Interpolant
Secret launch Code

- We have a unique solution:

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 65172 \\ 205061 \\ 197312 \\ 244235 \end{bmatrix}$$

- Plug in our coefficients:

$$P(x)$$
$$= 65172 + 205061(x-1) + 197312(x-1)(x-2)$$
$$+ 244235(x-1)(x-2)(x-4) \ (mod\ 319993)$$

- Gather Like terms:

$$Constant\ Term\ of\ P(x) = 220813 = "WIN"$$

Newton Interpolant
Secret launch Code

- Take a look at the **Newton** matrix equation:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 3 & 6 & 0 \\ 1 & 7 & 42 & 168 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 65172 \\ 270233 \\ 264262 \\ 260289 \end{bmatrix}$$

- Compared to the matrix equation from a **standard basis**:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \\ 1 & 4 & 16 & 64 \\ 1 & 8 & 64 & 512 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} = \begin{bmatrix} 65172 \\ 270233 \\ 264262 \\ 260289 \end{bmatrix}$$

Sources

- http://www.csmonitor.com/var/ezflow_site/storage/images/media/content/2012/0111-clock/11434734-1-eng-US/0111-clock_full_600.jpg
- http://www.thebulletin.org/content/doomsday-clock/timeline
- http://www.nytimes.com/2010/10/28/technology/28compute.html
- Trappe, Wade and Laurence Washington. *Introduction to Cryptography with Coding Theory. Pierson Education, inc. NJ, 2006.*