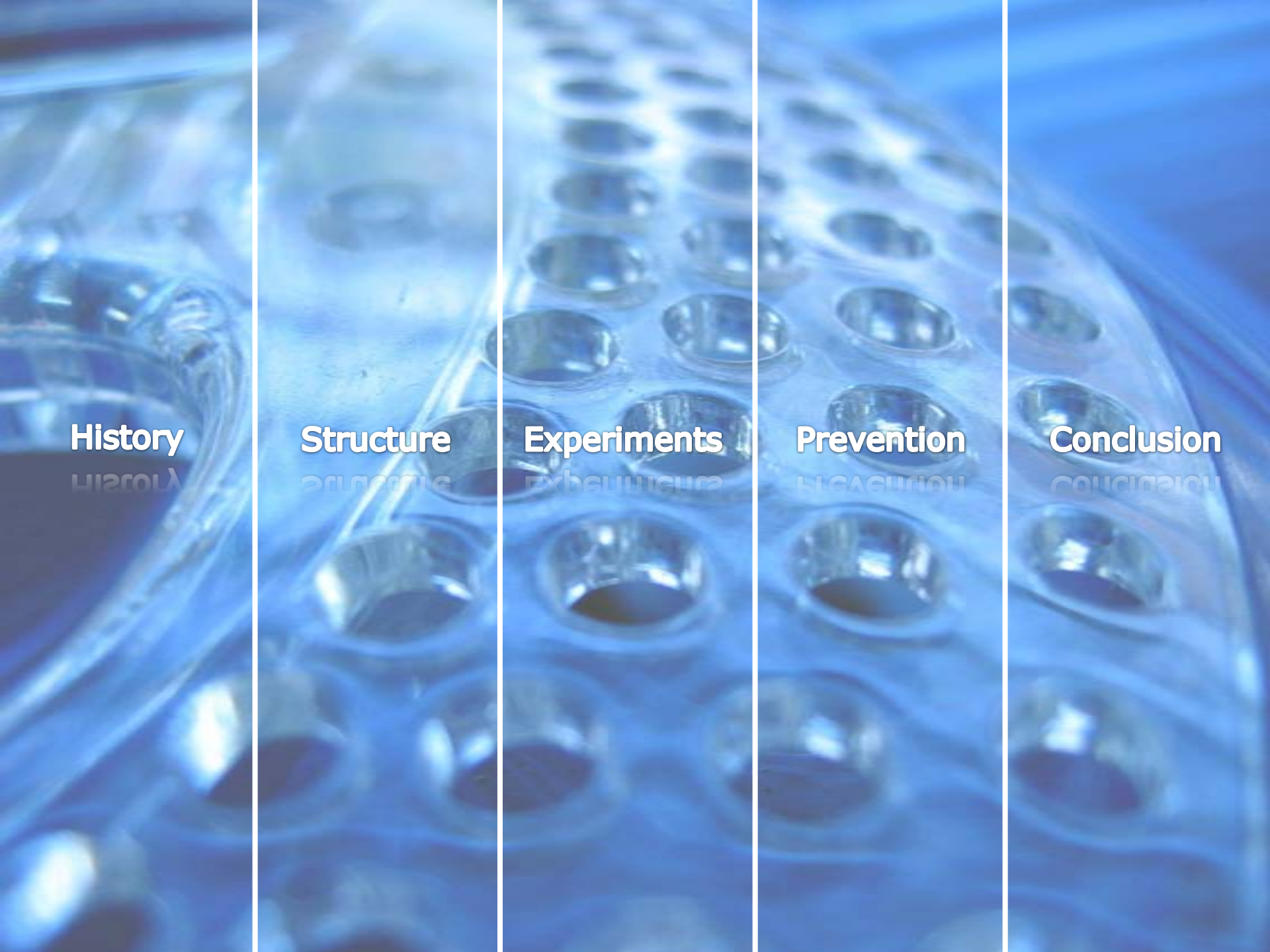
H.K. Jørgensen & R. Norbutaite

Rainbow tables

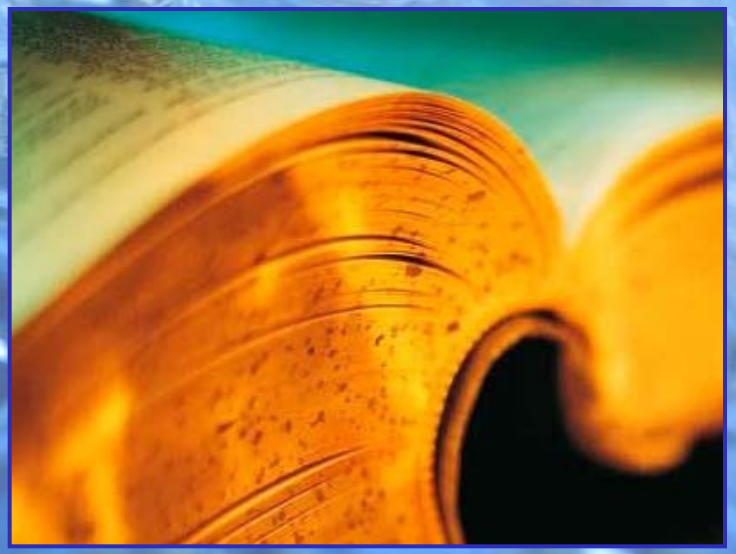
January 11, 2008

Cryptography


History
Structure
Experiments
Prevention
Conclusion

Relevant concepts

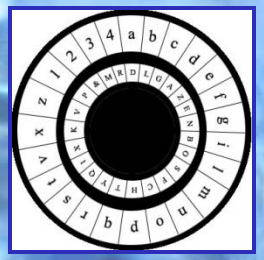
Brute-force



Dictionaries

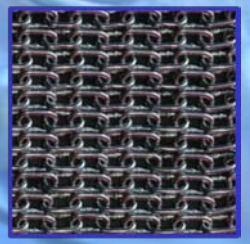
History

Hellman's Method



All possible cipher texts and keys

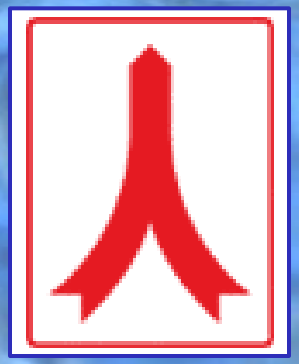
Organizing chains



Finding the right key

Collisions, Merges and False Alarms

From the space of cipher texts to the space of keys



Did we find the key?

Optimisation by Rivest

Distinguished points

Structure

Structure of Rainbow Tables

Presented by Oechslin

Aim: To diminish the merges!

Advantages of DP

- Reduced look ups
- Detectable merges
- No loops

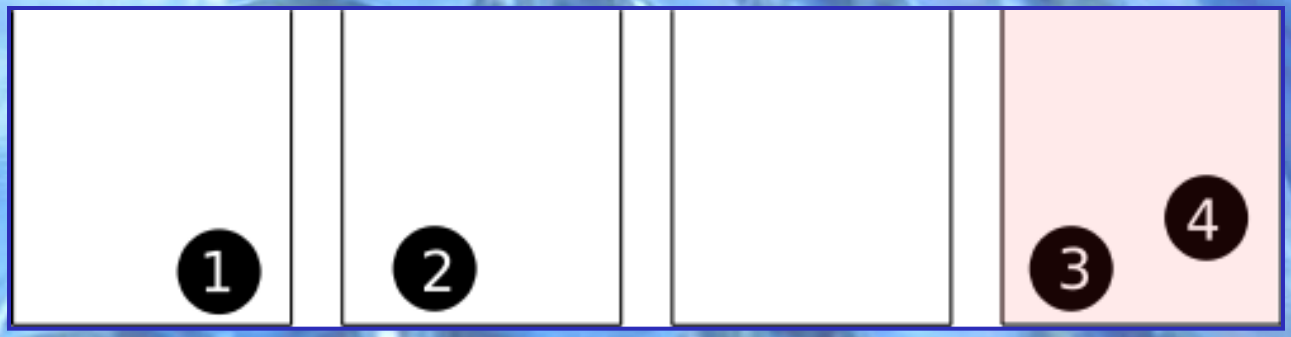
Why Fixed Length?

Fatal attraction

Larger overhead

The Success Rate

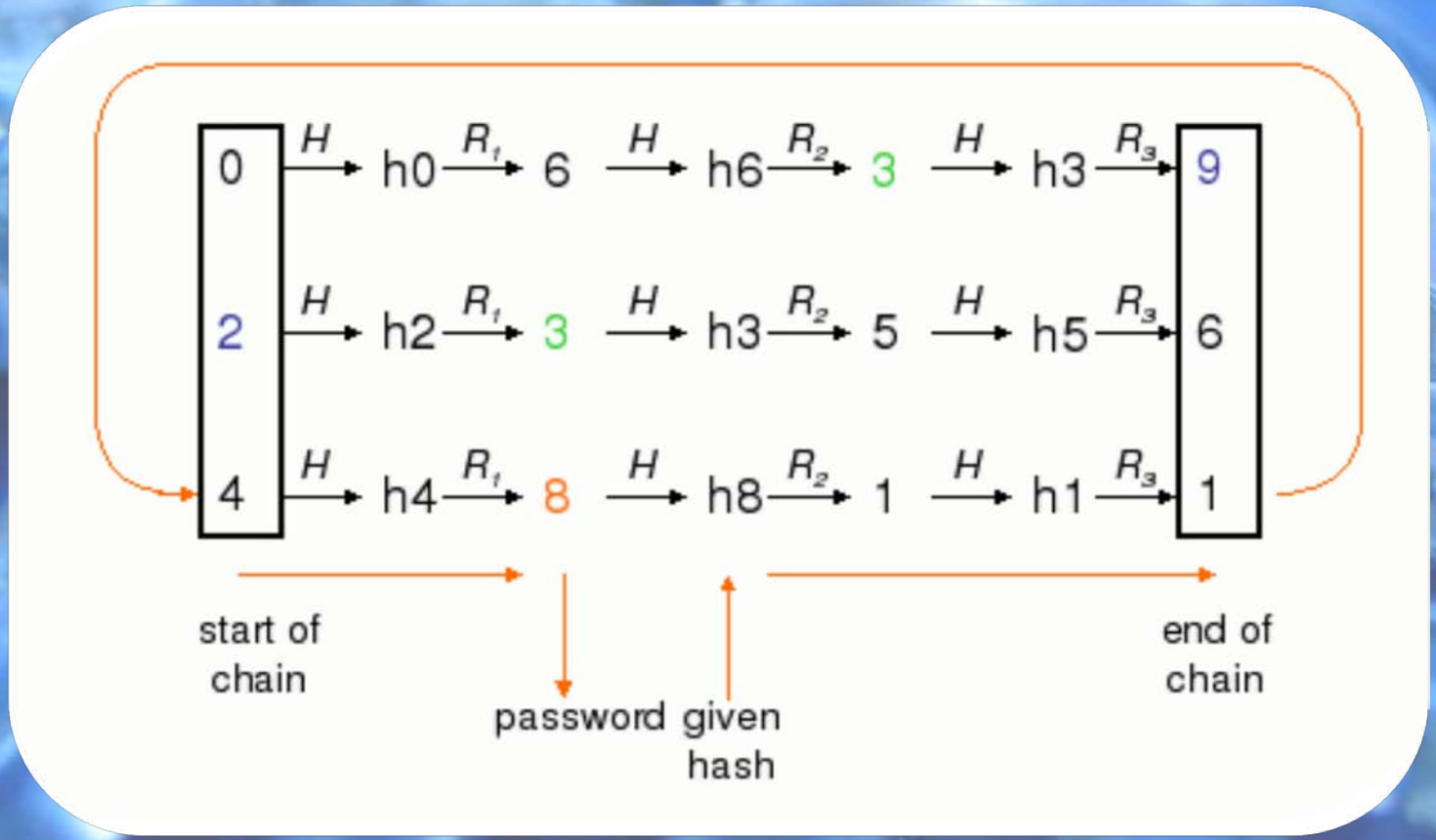
Occupancy Problem



$$P = 1 - \prod_{i=1}^{t} (1 - \frac{m_i}{N})$$

The Chance of Success

How to use the Table



Going backward in a one-way function

Experiments

LanManager Experiment

14 character password

7 first characters	**7 last characters**
7 FIRST CHARACTERS	**7 LAST CHARACTERS**

DES(p,k**)**

DES(KGS!@#$%,k**)**

LanManager Experiment

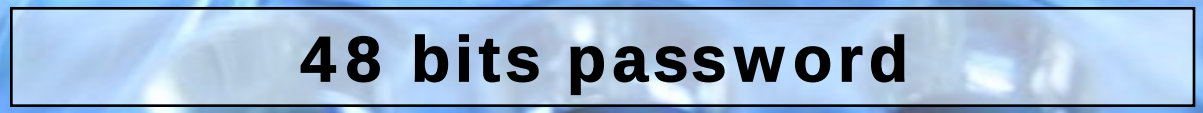
	classic with DP	rainbow
t, m, ℓ	4666, 8192, 4666	4666, 38'223'872, 1
predicted coverage	75.5%	77.5%
measured coverage	75.8%	78.8%

	classic with DP	rainbow	ratio
t, m, ℓ	4666, 8192, 4666	4666, 38'223'872, 1	1
	mean cryptanalysis time		
to success	68.9s	9.37s	7.4
to failure	181.0s	26.0s	7.0
average	96.1s	12.9s	7.4
	mean nbr of hash calculations		
to success	48.3M	6.77M	7.1
to failure	126M	18.9M	6.7
average	67.2M	9.34M	7.2

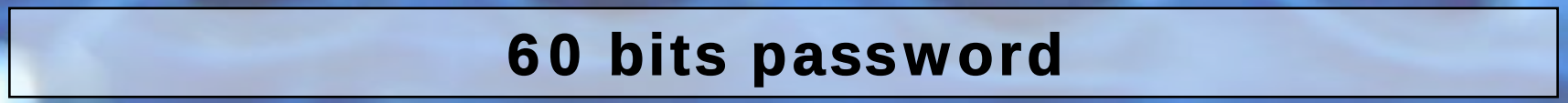
	mean nbr of false alarms		
to success	4157	1492	2.8
to failure	10913	5166	2.1
average	5792	2271	2.6
	mean nbr of hash calculations per false alarms		
to success	9622	3030	3.2
to failure	9557	1551	6.2
average	9607	2540	3.8

Unix Experiment

Salt is known and is not unique

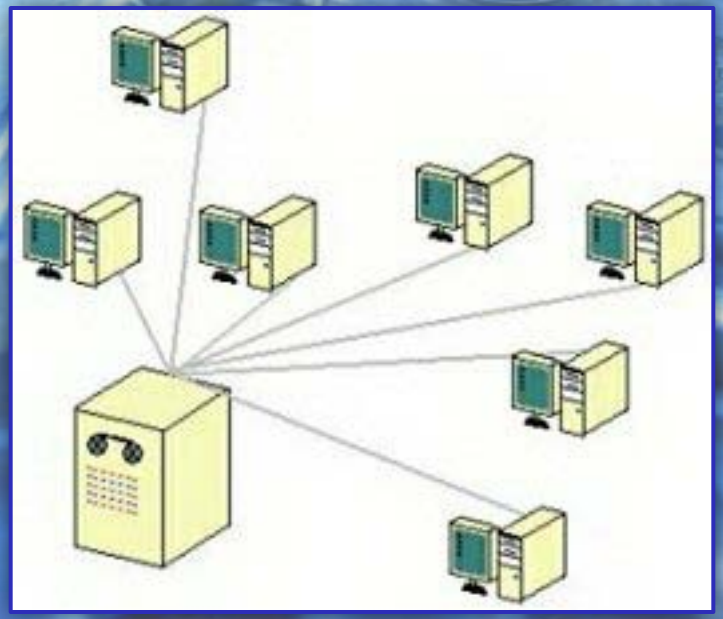


Salt is unique



Generalised Version

Zhu Shuanglei

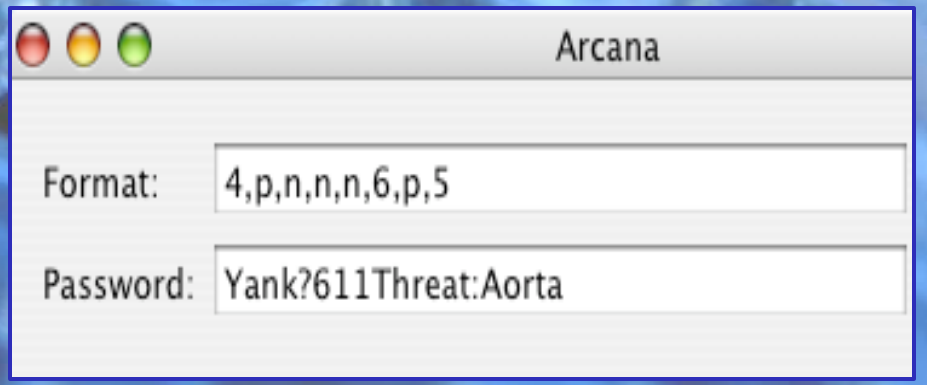


Distributed Computing

Prevention

Prevention

Salt

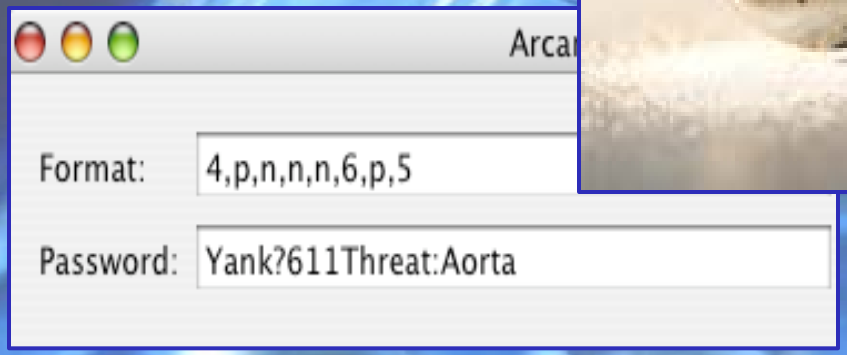


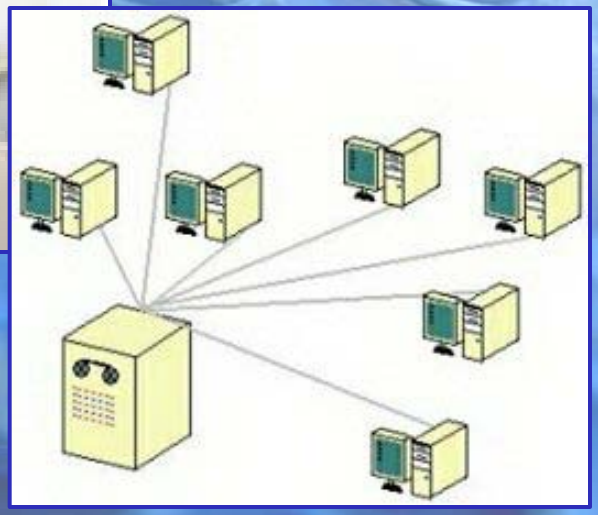
Long passwords

Conclusion

Conclusion

Efficient, but can be prevented





Be aware of distributed effort