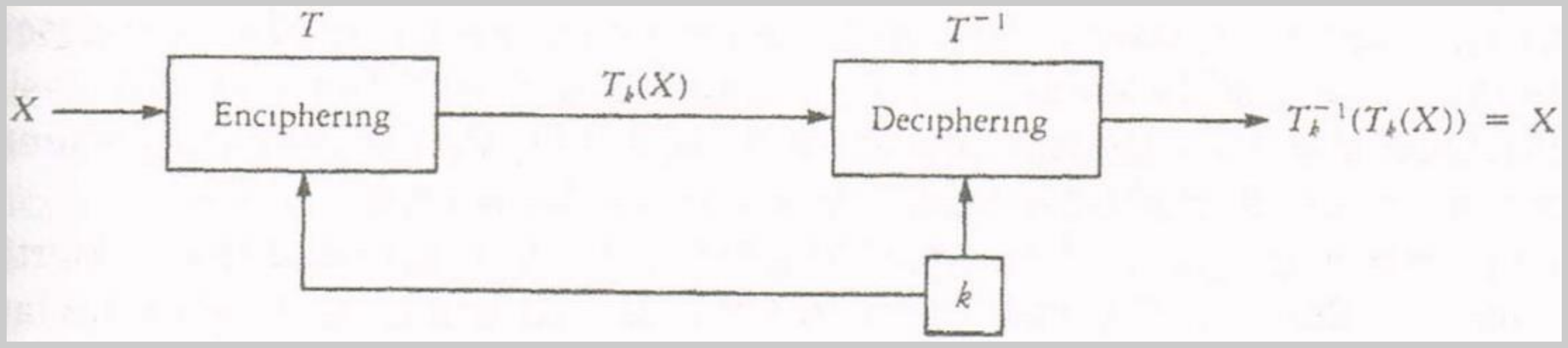
July 2015

Public Key Cryptography

Jordan Spooner

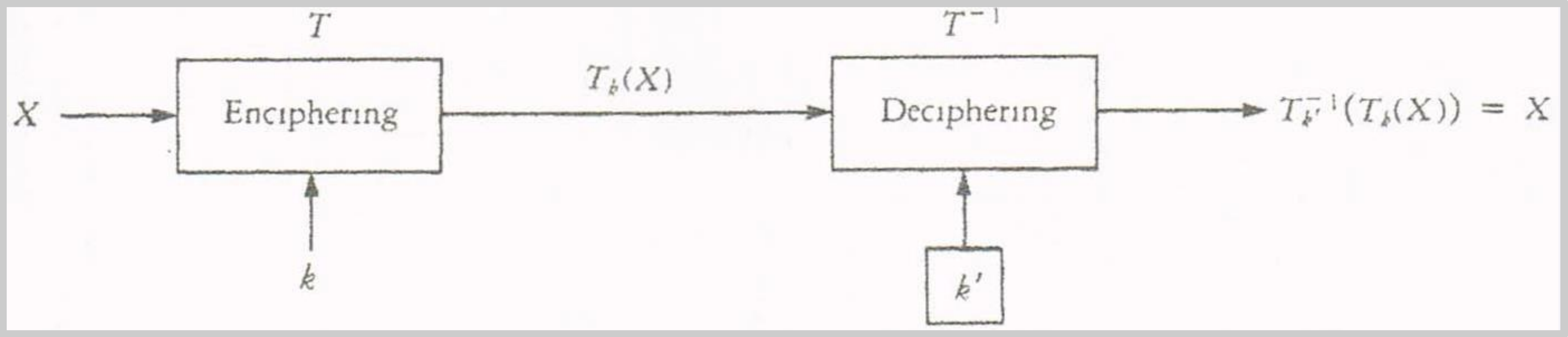
Cryptography

1. Traditional Encryption



Cryptography

2. Public Key Encryption



The Subset Sum Problem

Given $n+1$ positive integers, $a_1, a_2, \ldots, a_n$ and B, find a subset of the a_i that sums to B

Encrypting a Message

- Public key:, $a_1, a_2, \ldots, a_n$
- Character in Message: x, transformed to Blocks of length n, $(x_1, x_2, \ldots, x_n)$
- Output: $B_x = \sum_{i=1}^{n} x_i a_i$

An Example of Encryption

S	E	C	R	E	T
1010011	1000101	1000011	1010010	1000101	1010100

Decrypting the Message

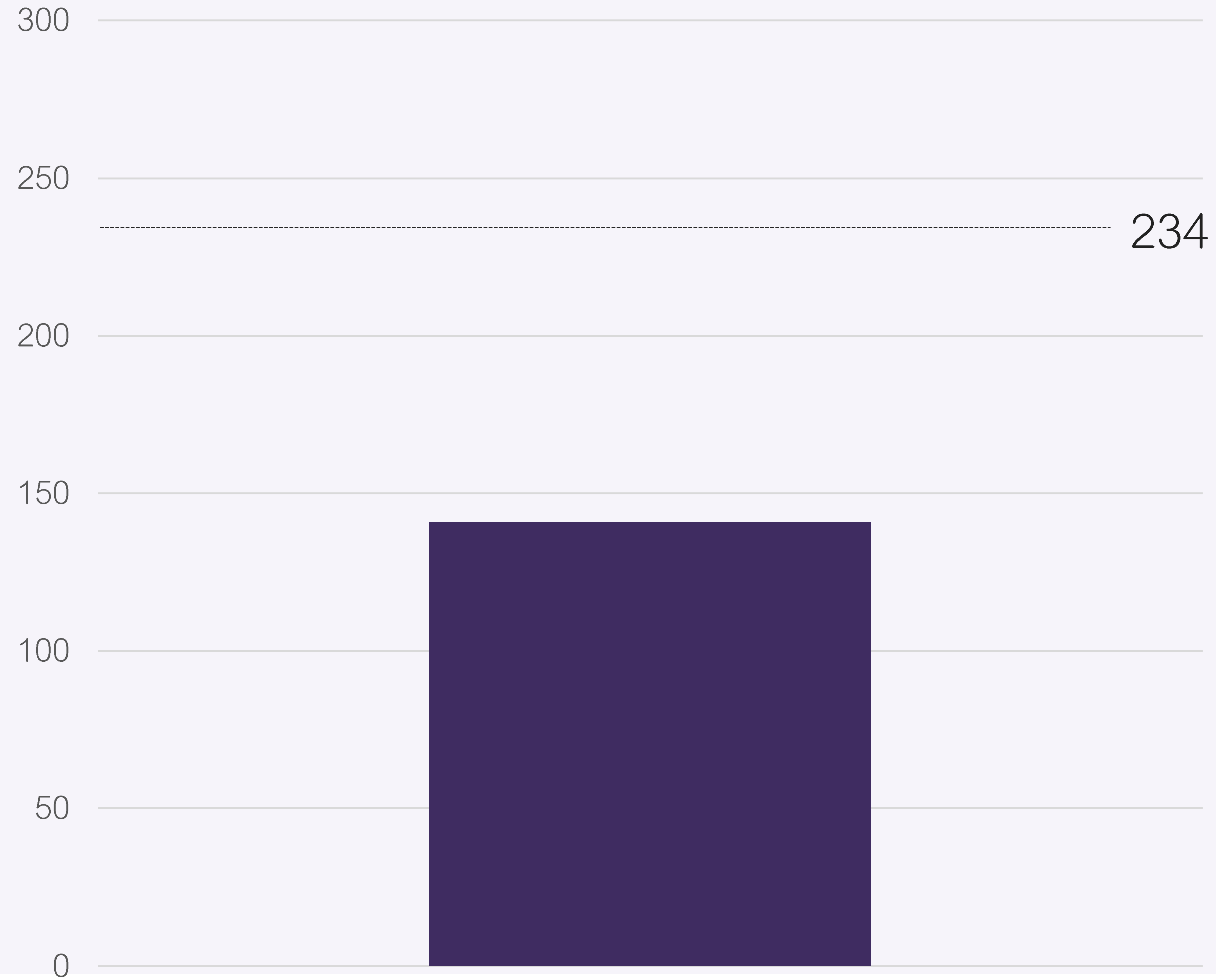
- Private key: $(a'_1, a'_2, \ldots, a'_n)$ and two integers, w and m
- Public and Private Keys related:

$$a_i = (w \times a'_i) \bmod m$$

- Find a subset of $(a'_1, a'_2, \ldots, a'_n)$ that gives B'_x, where $B'_x = (B_x \times w^{-1}) \bmod m$
  - Take the largest integer, a'_n: if $B'_x > a'_n$, then include a'_n, else discard it
  - Take the next largest integer, a'_i, if $B'_x > \sum a'_{included} + a'_i$, then include a'_i, else discard it
  - Repeat the second step until $\sum a'_{included} = B'_x$

An Example of Decryption

An Example of Decryption



141

87

32

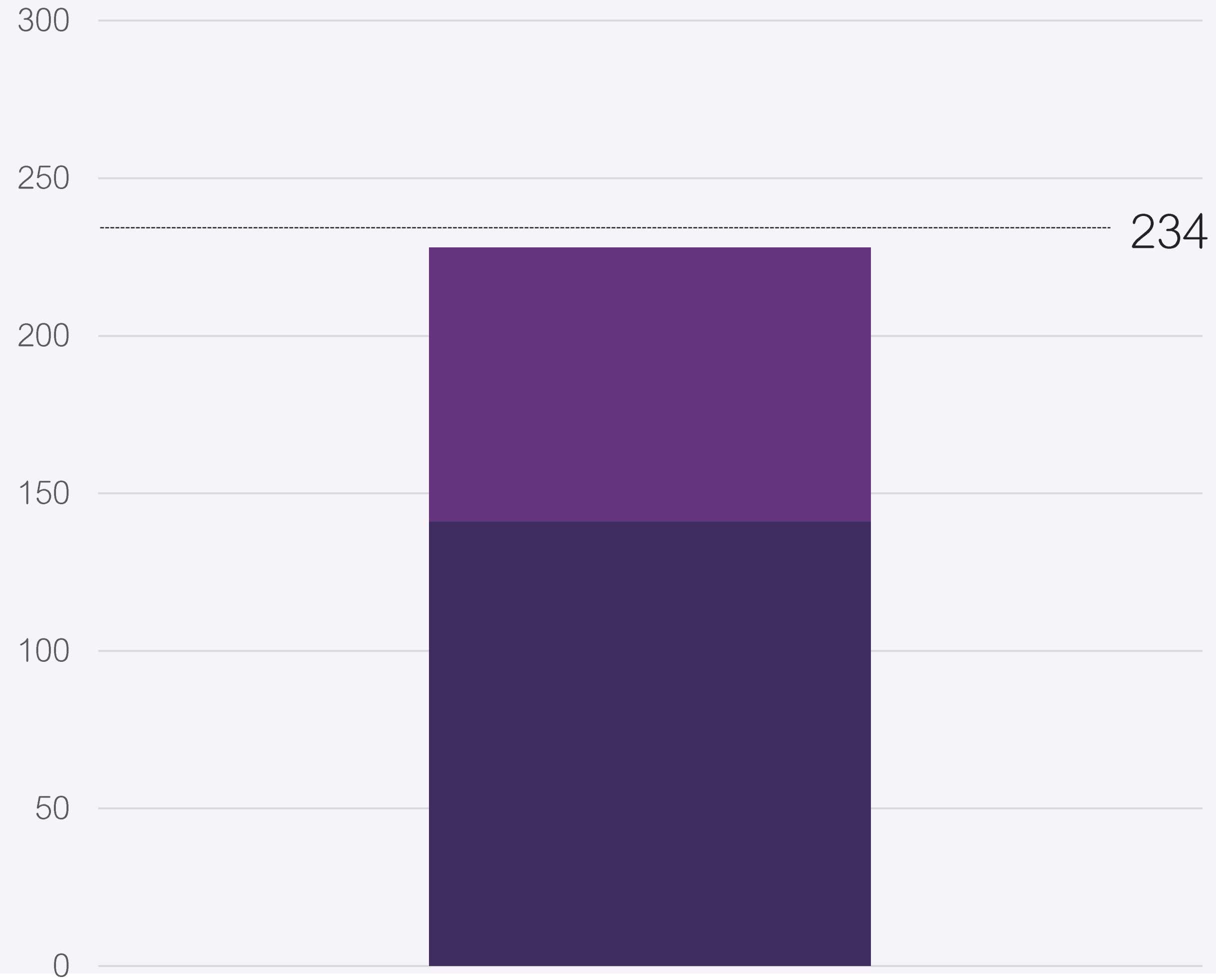
11

5

2

1

An Example of Decryption



141

87

32

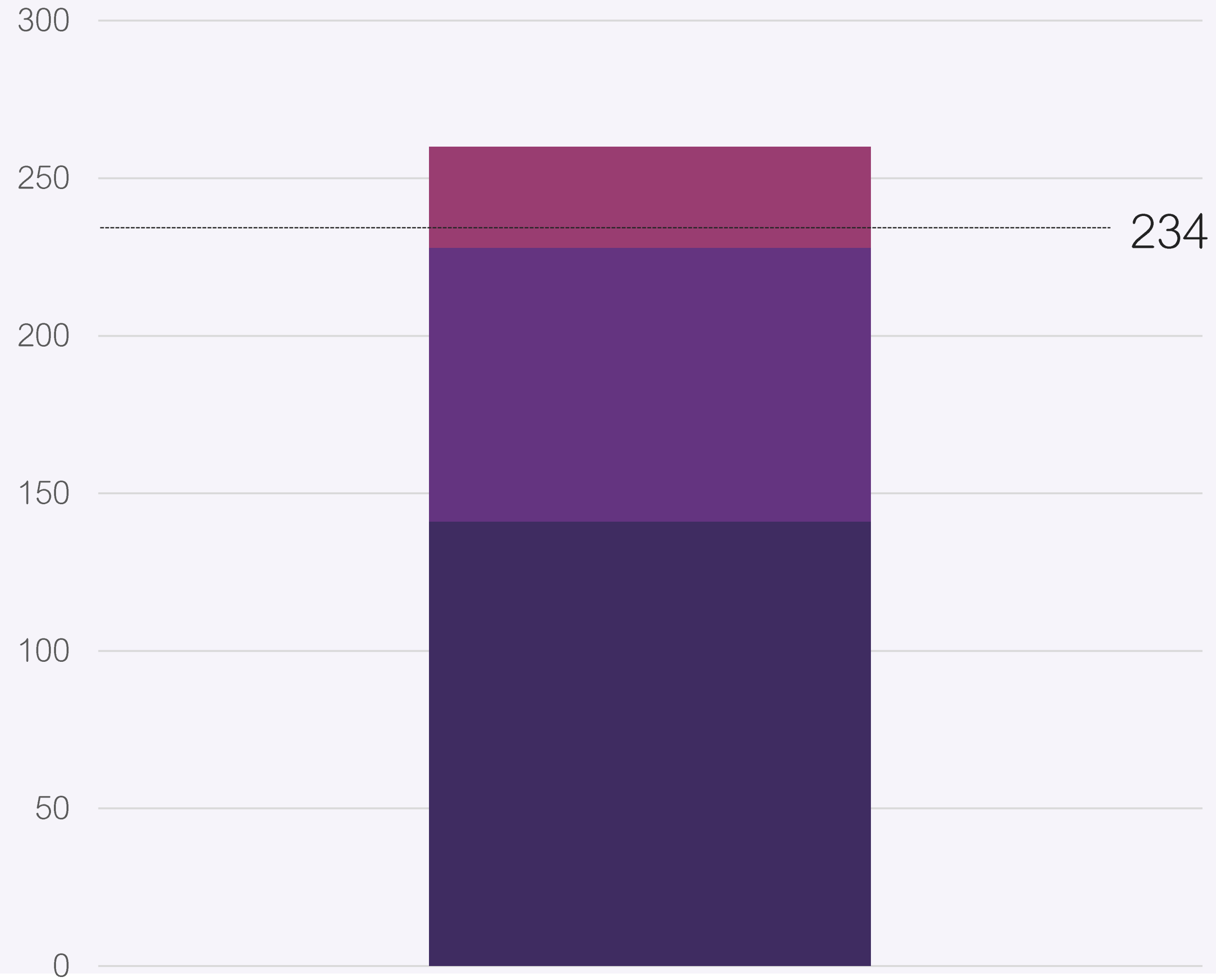
11

5

2

1

An Example of Decryption



141

87

32

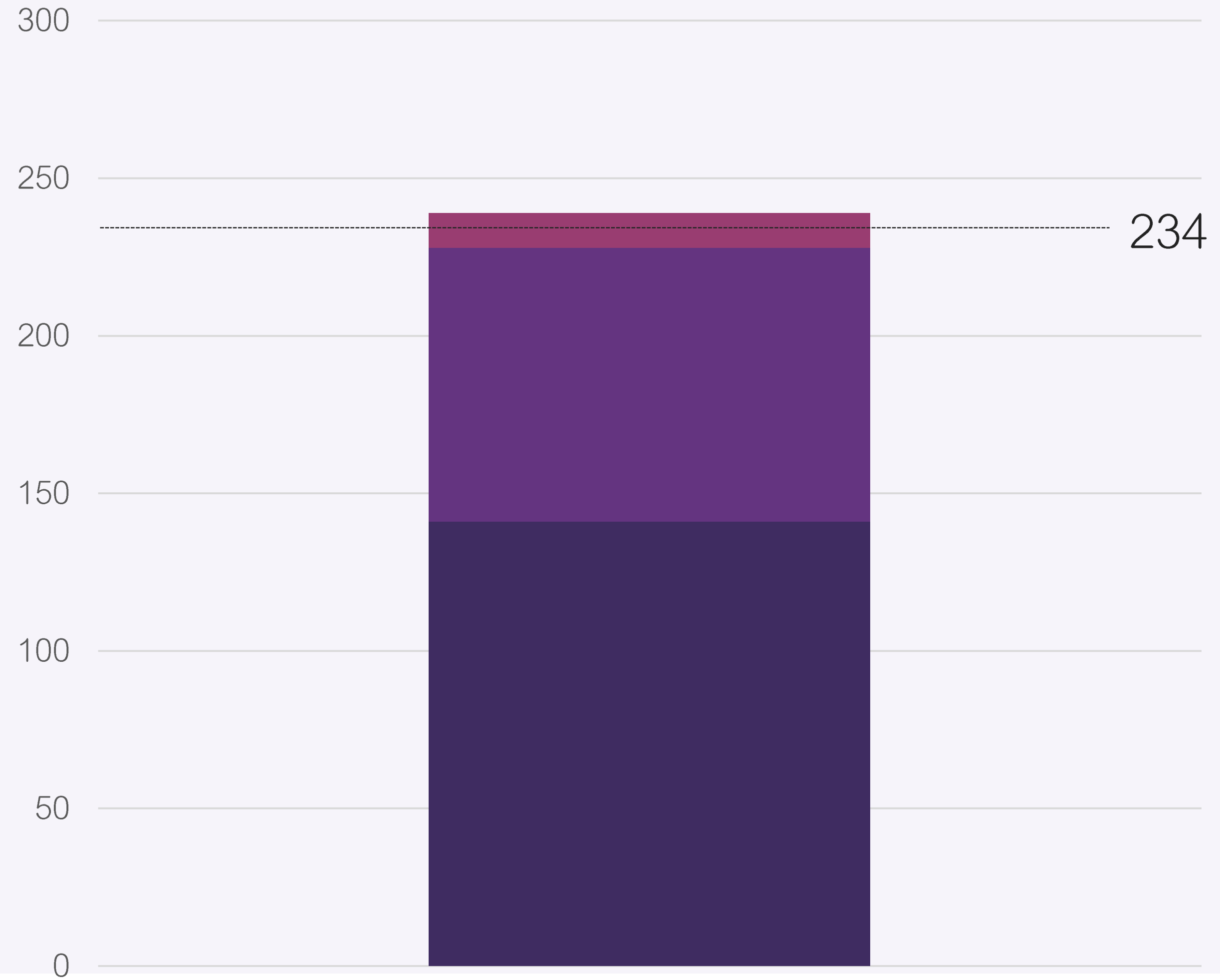
11

5

2

1

An Example of Decryption



141

87

~~32~~

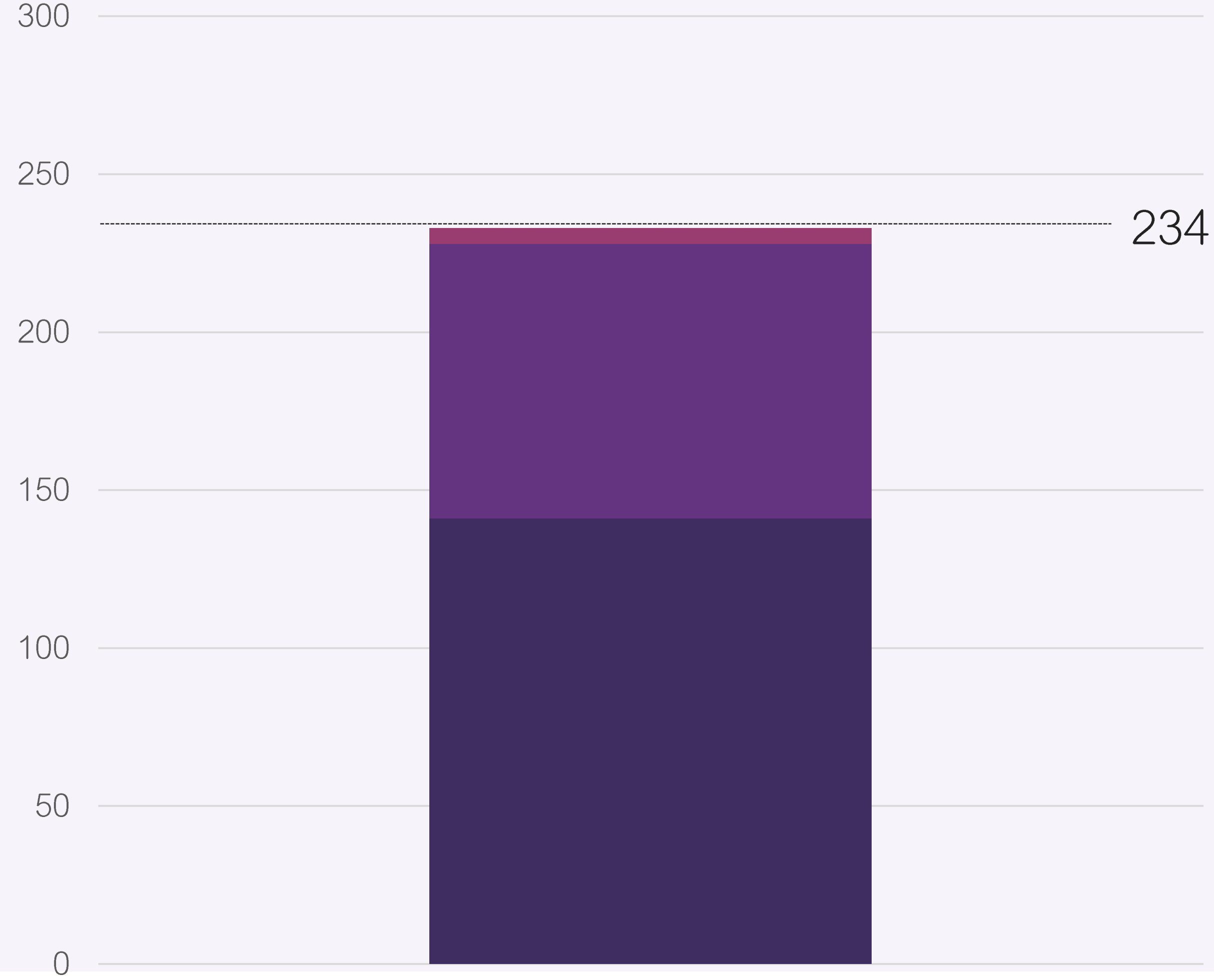
11

5

2

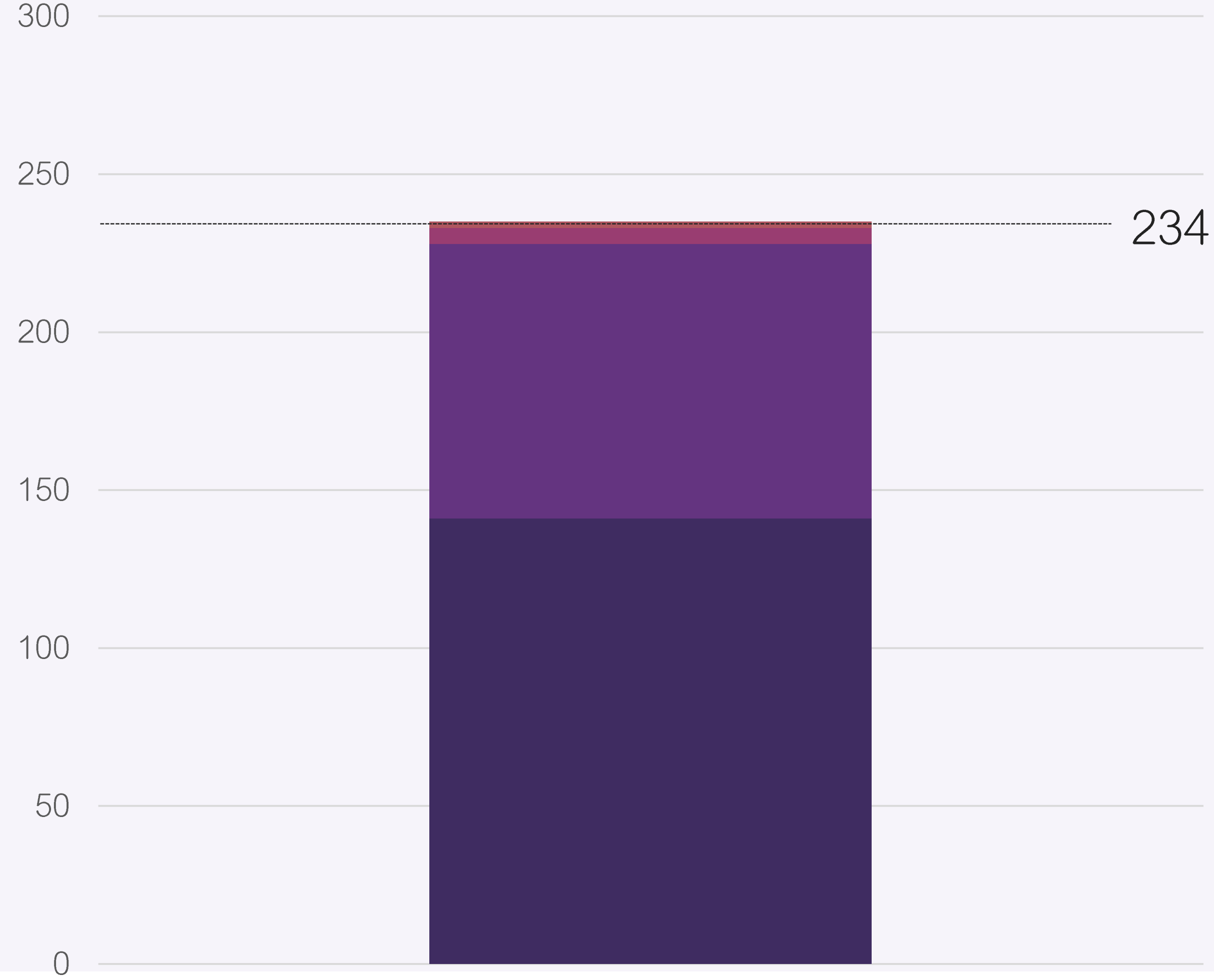
1

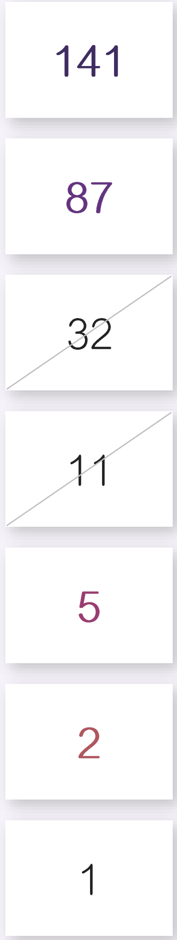
An Example of Decryption



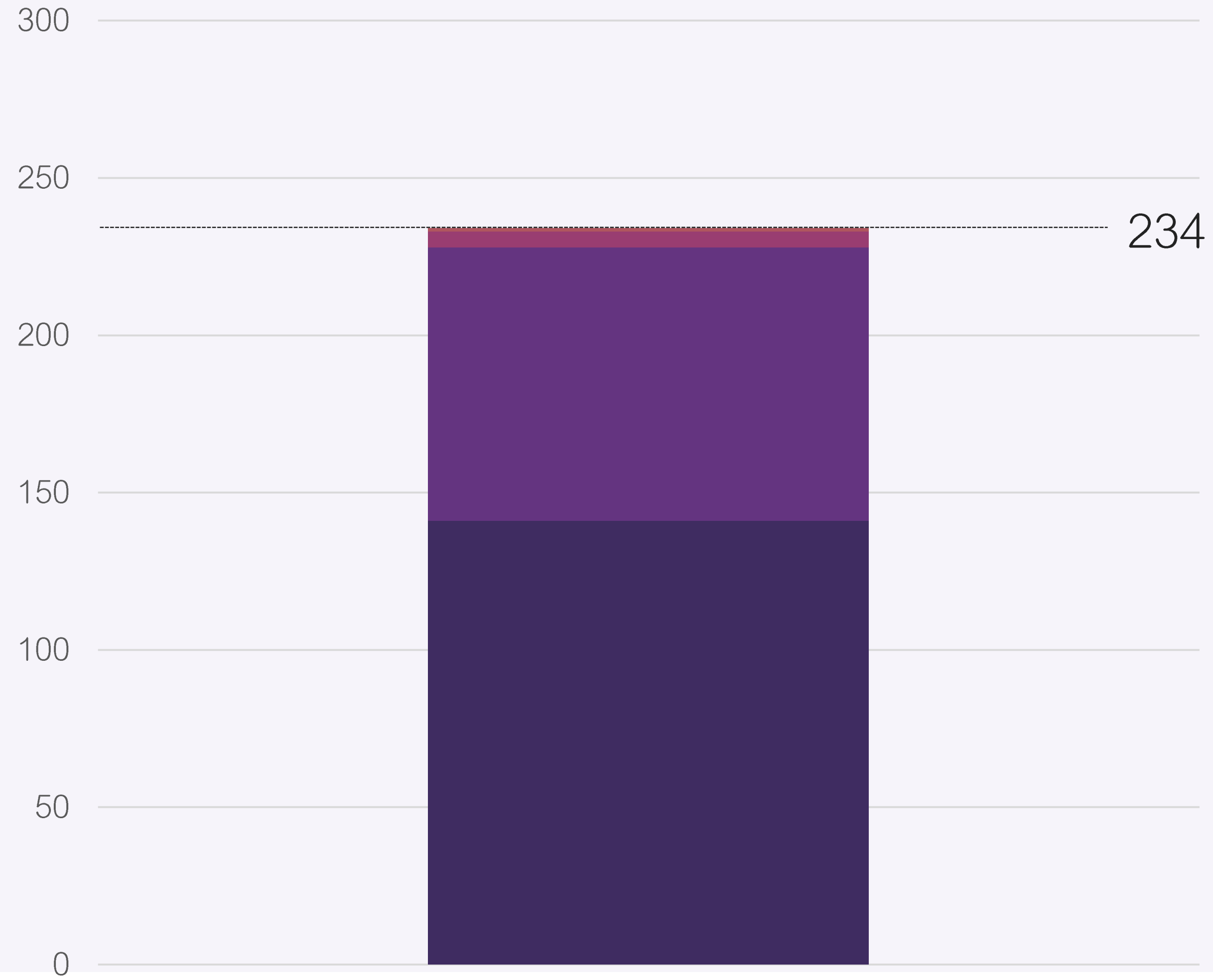
141
87
~~32~~
~~11~~
5
2
1

An Example of Decryption





An Example of Decryption



141

87

~~32~~

~~11~~

5

~~2~~

1

An Overview of How it Works

– Looking at T and T^{-1}:

T: $B_x = \sum_{i=1}^{n} x_i a_i = \sum_{i=1}^{n} x_i \times w a_i' \bmod m$

T^{-1}: $B_x' = (B_x \times w^{-1}) \bmod m$,

$B_x' = \sum_{i=1}^{n} x_i (w a_i' \bmod m)\, w^{-1} \bmod m$ and hence $B_x' = \sum_{i=1}^{n} x_i a_i'$

I.e. the message x encoded in B_x as $\sum_{i=1}^{n} x_i a_i$ is encoded in B_x' as $\sum_{i=1}^{n} x_i a_i'$

How to Break it?

- Points of Vulnerability
- The Diffie-Hellman-Merkle Cryptosystem
- The RSA Cryptosystem
- Quantum Computing and Shor’s Algorithm