A PRIME LOOK INTO THE FIELD OF CRYPTOGRAPHY

KRISTEN BRESSLER
kbressler@carroll.edu
Hello world!!!
Hello world!!! 11001010

Encoding

OVERVIEW
OVERVIEW

Hello world!!! → 11001010 → 10010011

Encryption + PUB

PRIV
Hello world!!! 11001010 10010011 → 📣
Hello world!!!
OVERVIEW

Hello world!!!

1101010 → 10010011 → 10010011 → 10010011 → 1101010

Decryption +

PRIV

PUB
RSA
### RSA

<table>
<thead>
<tr>
<th>Public Key</th>
<th>Private Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n: n = pq )</td>
<td>( p: ) a large prime number</td>
</tr>
<tr>
<td>( e: ) coprime to ( \phi(n) )</td>
<td>( q: ) a large prime number</td>
</tr>
</tbody>
</table>
|                     | \( d: \) multiplicative inverse of \( e \mod n \)

Encryption Algorithm: \( E(m, pub) = E(m, (n, e)) = m^e (\mod n) = c \)

Decryption Algorithm: \( D(m, priv) = D(m, (n, d)) = c^d (\mod n) = m \)
ELLIPTIC CURVE
ELLIPITC CURVE

\[ y^2 = x^3 + ax + b \]
ELLiptic Curve - EncryPTION
THANK YOU!