Disc 3a

Andy

UC Berkeley

July 1, 2018

Implications of RSA

1. 2 people can communicate securely despite eavesdroppers!

Implications of RSA

1. 2 people can communicate securely despite eavesdroppers!
2. Eavesdropper CANNOT decipher the conversation

Implications of RSA

1. 2 people can communicate securely despite eavesdroppers!
2. Eavesdropper CANNOT decipher the conversation
3. RSA is hard because factoring is ... hard?

Implications of RSA

1. 2 people can communicate securely despite eavesdroppers!
2. Eavesdropper CANNOT decipher the conversation
3. RSA is hard because factoring is ... hard?
4. No one has proven factoring is hard

Implications of RSA

1. 2 people can communicate securely despite eavesdroppers!
2. Eavesdropper CANNOT decipher the conversation
3. RSA is hard because factoring is ... hard?
4. No one has proven factoring is hard
5. If you figured out factoring was hard, what would you do?

Implications of RSA

1. 2 people can communicate securely despite eavesdroppers!
2. Eavesdropper CANNOT decipher the conversation
3. RSA is hard because factoring is ... hard?
4. No one has proven factoring is hard
5. If you figured out factoring was hard, what would you do?
6. Keep it secret to yourself? But other people might be mean

Implications of RSA

1. 2 people can communicate securely despite eavesdroppers!
2. Eavesdropper CANNOT decipher the conversation
3. RSA is hard because factoring is ... hard?
4. No one has proven factoring is hard
5. If you figured out factoring was hard, what would you do?
6. Keep it secret to yourself? But other people might be mean
7. Tell the US govt. Get taken out by the CIA.

Implications of RSA

1. 2 people can communicate securely despite eavesdroppers!
2. Eavesdropper CANNOT decipher the conversation
3. RSA is hard because factoring is ... hard?
4. No one has proven factoring is hard
5. If you figured out factoring was hard, what would you do?
6. Keep it secret to yourself? But other people might be mean
7. Tell the US govt. Get taken out by the CIA.
8. Tell the world, crash online banking, online security, in minutes.

Implications of RSA

1. 2 people can communicate securely despite eavesdroppers!
2. Eavesdropper CANNOT decipher the conversation
3. RSA is hard because factoring is ... hard?
4. No one has proven factoring is hard
5. If you figured out factoring was hard, what would you do?
6. Keep it secret to yourself? But other people might be mean
7. Tell the US govt. Get taken out by the CIA.
8. Tell the world, crash online banking, online security, in minutes.
9. Its a cool hypothetical

Implications of RSA

1. 2 people can communicate securely despite eavesdroppers!
2. Eavesdropper CANNOT decipher the conversation
3. RSA is hard because factoring is ... hard?
4. No one has proven factoring is hard
5. If you figured out factoring was hard, what would you do?
6. Keep it secret to yourself? But other people might be mean
7. Tell the US govt. Get taken out by the CIA.
8. Tell the world, crash online banking, online security, in minutes.
9. Its a cool hypothetical
10. Do let me know if you figure out factoring though!

Minilecture: Interpolation

1. I want a function that's

Minilecture: Interpolation

1. I want a function that's
2. $f(4) = 5$, $f(7) = 10$, $f(2) = 5$.

Minilecture: Interpolation

1. I want a function that's
2. $f(4) = 5$, $f(7) = 10$, $f(2) = 5$.
3. $\Delta_4(4) = 1$, $d(i) = 0 \forall i, i \neq 4$

Minilecture: Interpolation

1. I want a function that's
2. $f(4) = 5,\ f(7) = 10,\ f(2) = 5.$
3. $\Delta_4(4) = 1,\ d(i) = 0 \forall i, i \neq 4$
4. $\Delta_7(7) = 1,\ d(i) = 0 \forall i, i \neq 7$

Minilecture: Interpolation

1. I want a function that's
2. $f(4) = 5,\ f(7) = 10,\ f(2) = 5.$
3. $\Delta_4(4) = 1,\ d(i) = 0 \forall i, i \neq 4$
4. $\Delta_7(7) = 1,\ d(i) = 0 \forall i, i \neq 7$
5. $\Delta_2(2) = 1,\ d(i) = 0 \forall i, i \neq 2$

Minilecture: Interpolation

1. I want a function that's
2. $f(4) = 5$, $f(7) = 10$, $f(2) = 5$.
3. $\Delta_4(4) = 1$, $d(i) = 0 \forall i, i \neq 4$
4. $\Delta_7(7) = 1$, $d(i) = 0 \forall i, i \neq 7$
5. $\Delta_2(2) = 1$, $d(i) = 0 \forall i, i \neq 2$
6. How does this help?

Minilecture: Interpolation

1. I want a function that's
2. $f(4) = 5$, $f(7) = 10$, $f(2) = 5$.
3. $\Delta_4(4) = 1$, $d(i) = 0 \forall i, i \neq 4$
4. $\Delta_7(7) = 1$, $d(i) = 0 \forall i, i \neq 7$
5. $\Delta_2(2) = 1$, $d(i) = 0 \forall i, i \neq 2$
6. How does this help?
7. $f(x) = 5 * \Delta_4(x) + 10 * \Delta_7(x) + 5 * \Delta_2(x)$

Minilecture: Interpolation

1. I want a function that's
2. $f(4) = 5,\ f(7) = 10,\ f(2) = 5.$
3. $\Delta_4(4) = 1,\ d(i) = 0 \forall i, i \neq 4$
4. $\Delta_7(7) = 1,\ d(i) = 0 \forall i, i \neq 7$
5. $\Delta_2(2) = 1,\ d(i) = 0 \forall i, i \neq 2$
6. How does this help?
7. $f(x) = 5 * \Delta_4(x) + 10 * \Delta_7(x) + 5 * \Delta_2(x)$
8. Sanity Check:
   $f(4) = 5 = 5 * \Delta_4(4) + 10 * \Delta_7(4) + 5 * \Delta_2(4)$

Minilecture: Interpolation

1. I want a function that's
2. $f(4) = 5$, $f(7) = 10$, $f(2) = 5$.
3. $\Delta_4(4) = 1$, $d(i) = 0 \forall i, i \neq 4$
4. $\Delta_7(7) = 1$, $d(i) = 0 \forall i, i \neq 7$
5. $\Delta_2(2) = 1$, $d(i) = 0 \forall i, i \neq 2$
6. How does this help?
7. $f(x) = 5 * \Delta_4(x) + 10 * \Delta_7(x) + 5 * \Delta_2(x)$
8. Sanity Check:
   $f(4) = 5 = 5 * \Delta_4(4) + 10 * \Delta_7(4) + 5 * \Delta_2(4)$
9. Sanity Check: $f(4) = 5 = 5 * 1 + 10 * 0 + 5 * 0$

Minilecture: Interpolation

1. I want a function that's
2. $f(4) = 5,\ f(7) = 10,\ f(2) = 5.$
3. $\Delta_4(4) = 1,\ d(i) = 0 \forall i, i \neq 4$
4. $\Delta_7(7) = 1,\ d(i) = 0 \forall i, i \neq 7$
5. $\Delta_2(2) = 1,\ d(i) = 0 \forall i, i \neq 2$
6. How does this help?
7. $f(x) = 5 * \Delta_4(x) + 10 * \Delta_7(x) + 5 * \Delta_2(x)$
8. Sanity Check:
   $f(4) = 5 = 5 * \Delta_4(4) + 10 * \Delta_7(4) + 5 * \Delta_2(4)$
9. Sanity Check: $f(4) = 5 = 5 * 1 + 10 * 0 + 5 * 0$
10. $\Delta_i(x)$ is called a Delta function

1. Count and Prove

1. CRT says a solution exists within $[0, 105)$

1. Count and Prove

1. CRT says a solution exists within $[0, 105)$
2. I need something that is 1 mod 3, 0 mod 5, 0 mod 7

1. Count and Prove

1. CRT says a solution exists within $[0, 105)$
2. I need something that is 1 mod 3, 0 mod 5, 0 mod 7
3. $y_1 = (5 * 7) * ((5 * 7)^{-1} mod 3) = 35 * 2 = 70.$

1. Count and Prove

1. CRT says a solution exists within $[0, 105)$
2. I need something that is 1 mod 3, 0 mod 5, 0 mod 7
3. $y_1 = (5 * 7) * ((5 * 7)^{-1} mod 3) = 35 * 2 = 70.$
4. Check: $35 \equiv 1$ mod 3. $35 \equiv 0$ mod 5. $35 \equiv 0$ mod 7.

1. Count and Prove

1. CRT says a solution exists within $[0, 105)$
2. I need something that is 1 mod 3, 0 mod 5, 0 mod 7
3. $y_1 = (5 * 7) * ((5 * 7)^{-1} mod 3) = 35 * 2 = 70.$
4. Check: $35 \equiv 1$ mod 3. $35 \equiv 0$ mod 5. $35 \equiv 0$ mod 7.
5. $y_2 = (3 * 7) * ((3 * 7)^{-1} mod 5) = 21$

1. Count and Prove

1. CRT says a solution exists within $[0, 105)$
2. I need something that is 1 mod 3, 0 mod 5, 0 mod 7
3. $y_1 = (5 * 7) * ((5 * 7)^{-1} mod 3) = 35 * 2 = 70.$
4. Check: $35 \equiv 1$ mod 3. $35 \equiv 0$ mod 5. $35 \equiv 0$ mod 7.
5. $y_2 = (3 * 7) * ((3 * 7)^{-1} mod 5) = 21$
6. $y_3 = (3 * 5) * ((3 * 5)^{-1} mod 7) = 15$

1. Count and Prove

1. CRT says a solution exists within $[0, 105)$
2. I need something that is 1 mod 3, 0 mod 5, 0 mod 7
3. $y_1 = (5 * 7) * ((5 * 7)^{-1} mod 3) = 35 * 2 = 70.$
4. Check: $35 \equiv 1 \mod 3$. $35 \equiv 0 \mod 5$. $35 \equiv 0 \mod 7$.
5. $y_2 = (3 * 7) * ((3 * 7)^{-1} mod 5) = 21$
6. $y_3 = (3 * 5) * ((3 * 5)^{-1} mod 7) = 15$
7. $x = 2 * y_1 + 3 * y_2 + 4 * y_3 \mod 105$

1. Count and Prove

1. CRT says a solution exists within $[0, 105)$
2. I need something that is 1 mod 3, 0 mod 5, 0 mod 7
3. $y_1 = (5 * 7) * ((5 * 7)^{-1} mod 3) = 35 * 2 = 70.$
4. Check: $35 \equiv 1 \bmod 3$. $35 \equiv 0 \bmod 5$. $35 \equiv 0 \bmod 7$.
5. $y_2 = (3 * 7) * ((3 * 7)^{-1} mod 5) = 21$
6. $y_3 = (3 * 5) * ((3 * 5)^{-1} mod 7) = 15$
7. $x = 2 * y_1 + 3 * y_2 + 4 * y_3 \bmod 105$
8. $x \equiv 263 \equiv 53 \bmod 105$

1. Count and Prove

1. Prove $n^{80} \equiv 1 \bmod 935$, then $5, 11, 17 \nmid n$.

1. Count and Prove

1. Prove $n^{80} \equiv 1 \bmod 935$, then $5, 11, 17 \nmid n$.
2. $n^{80} \equiv 1$ means $n^{80} = 935k + 1$ for some k.

1. Count and Prove

1. Prove $n^{80} \equiv 1 \bmod 935$, then $5, 11, 17 \nmid n$.
2. $n^{80} \equiv 1$ means $n^{80} = 935k + 1$ for some k.
3. $n^{80} \equiv 1 \bmod 5$

1. Count and Prove

1. Prove $n^{80} \equiv 1 \bmod 935$, then $5, 11, 17 \nmid n$.
2. $n^{80} \equiv 1$ means $n^{80} = 935k + 1$ for some k.
3. $n^{80} \equiv 1 \bmod 5$
4. Proof by contradiction:

1. Count and Prove

1. Prove $n^{80} \equiv 1 \bmod 935$, then $5, 11, 17 \nmid n$.
2. $n^{80} \equiv 1$ means $n^{80} = 935k + 1$ for some k.
3. $n^{80} \equiv 1 \bmod 5$
4. Proof by contradiction:
5. Assume $5 \mid n$, then $n = 5j$, which means $n \equiv 0 \pmod 5$.

1. Count and Prove

1. Prove $n^{80} \equiv 1 \bmod 935$, then $5, 11, 17 \nmid n$.
2. $n^{80} \equiv 1$ means $n^{80} = 935k + 1$ for some k.
3. $n^{80} \equiv 1 \bmod 5$
4. Proof by contradiction:
5. Assume $5 \mid n$, then $n = 5j$, which means $n \equiv 0 \pmod 5$.
6. Which means $n^{80} \equiv (5j)^{80} \equiv 0^{80} \equiv 0 \bmod 5$.

1. Count and Prove

1. Prove $n^{80} \equiv 1 \bmod 935$, then $5, 11, 17 \nmid n$.
2. $n^{80} \equiv 1$ means $n^{80} = 935k + 1$ for some k.
3. $n^{80} \equiv 1 \bmod 5$
4. Proof by contradiction:
5. Assume $5 \mid n$, then $n = 5j$, which means $n \equiv 0 \pmod 5$.
6. Which means $n^{80} \equiv (5j)^{80} \equiv 0^{80} \equiv 0 \bmod 5$.
7. Repeat for 11, 17.

1. $p(x) - q(x) = 0$. How many solutions to this?

2

1. $p(x) - q(x) = 0$. How many solutions to this?
2. How many degrees to $p - q$? At most $max(\Delta_1, \Delta_2)$

2

1. $p(x) - q(x) = 0$. How many solutions to this?
2. How many degrees to $p - q$? At most $max(\Delta_1, \Delta_2)$
3. $f(x) = (x - c)^2$, then $a = -2c$ and $b = c^2$, then $a^2 = 4c^2 = 4b$.

2

1. $p(x) - q(x) = 0$. How many solutions to this?
2. How many degrees to $p - q$? At most $max(\Delta_1, \Delta_2)$
3. $f(x) = (x - c)^2$, then $a = -2c$ and $b = c^2$, then $a^2 = 4c^2 = 4b$.
4. If f is even, 0. If f is odd, 1.

3

1. If f is even, 0. If f is odd, could be 0.

3

1. $P(x) = 4 * \Delta_1(x) + 3 * \Delta_2(x) + 0 * \Delta_5(x) \mod 7$

3

1. $P(x) = 4 * \Delta_1(x) + 3 * \Delta_2(x) + 0 * \Delta_5(x) \mod 7$
2. $\Delta_1(x) = \frac{(x-2)(x-5)}{(1-2)(1-5)} \mod 7$

3

1. $P(x) = 4 * \Delta_1(x) + 3 * \Delta_2(x) + 0 * \Delta_5(x) \bmod 7$
2. $\Delta_1(x) = \frac{(x-2)(x-5)}{(1-2)(1-5)} \bmod 7$
3. $\Delta_1(x) = \frac{(x-2)(x-5)}{4}$. Division in a modspace?

3

1. $P(x) = 4 * \Delta_1(x) + 3 * \Delta_2(x) + 0 * \Delta_5(x) \bmod 7$
2. $\Delta_1(x) = \frac{(x-2)(x-5)}{(1-2)(1-5)} \bmod 7$
3. $\Delta_1(x) = \frac{(x-2)(x-5)}{4}$. Division in a modspace?
4. $4^{-1} \equiv 2 \bmod 7$.

3

1. $P(x) = 4 * \Delta_1(x) + 3 * \Delta_2(x) + 0 * \Delta_5(x) \bmod 7$
2. $\Delta_1(x) = \frac{(x-2)(x-5)}{(1-2)(1-5)} \bmod 7$
3. $\Delta_1(x) = \frac{(x-2)(x-5)}{4}$. Division in a modspace?
4. $4^{-1} \equiv 2 \bmod 7$.
5. $\Delta_1(x) = 2 * (x-2)(x-5)$.

3

1. $P(x) = 4 * \Delta_1(x) + 3 * \Delta_2(x) + 0 * \Delta_5(x) \bmod 7$
2. $\Delta_1(x) = \frac{(x-2)(x-5)}{(1-2)(1-5)} \bmod 7$
3. $\Delta_1(x) = \frac{(x-2)(x-5)}{4}$. Division in a modspace?
4. $4^{-1} \equiv 2 \bmod 7$.
5. $\Delta_1(x) = 2 * (x-2)(x-5)$.
6. $P(x) \equiv 4(2x^2+6) + 3(2x^2+2x+3) \equiv 14x^2 + 6x + 33 \equiv 6x + 5 \bmod 7$