# RSA Encryption and Prime Factorization

People have needed to communicate information secretly for almost as long as we've been around. We can easily see how this can benefit finance or military, but it's even used in our day-to-day as computers communicate with each other. The earliest form of cryptography used what are known as **symmetric-key ciphers**, where two parties had access to a secret key that could both encrypt and decrypt messages. Of course, this requires the parties to have a way to communicate secretly in the first place. As technology advanced, the need for more sophisticated methods became necessary.

The RSA Cryptosystem—named after Ron Rivest, Adi Shamir, and Len Adleman, the first to publish[1] this method—is what is known as a **asymmetric-key cipher**, where everyone is allowed to encrypt with the public key, but only the holder of the private key can decrypt, making it great for one-way communications! While relatively new, it is built on notions, theorems, and work that has long existed in mathematics (we've covered most of it in class!).

RECALL: The **unit group** of $n$ is the set $\mathbb{Z}_n^\times := \{a \in \mathbb{Z}_n \mid a \text{ is a unit in } \mathbb{Z}_n\}$.

RECALL: Euler's phi function satisfies the following properties:

(1) If $p$ is prime and $n$ is a positive integer, then $\phi(p^n) = p^{(n-1)}(p-1)$.
(2) If $m, n$ are positive coprime integers, then $\phi(mn) = \phi(m)\phi(n)$.

(1) Generating an RSA Key:
   (a) Let $p = 47$ and $q = 59$. Calculate $n = pq$ and find $\phi(n)$.
   (b) Let $e = 17$. Explain why $e$ has an inverse modulo $\phi(n)$.
   (c) Find $d = e^{-1} \pmod{\phi(n)}$.

(2) Encoding and Encrypting:
   (a) Encode the message "HI" into an integer $m$ by converting the letters into numbers according to the table below and concatenating them in order.[2]

| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 |
| I | J | K | L | M | N | O | P | Q |
| 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| R | S | T | U | V | W | X | Y | Z |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

   (b) Find $y \equiv m^e \pmod{n}$.

(3) Decoding and Decrypting:
   (a) Find $x \equiv y^d \pmod{n}$ using any techniques[3] from class.
   (b) Decode $x$ into a message by reversing the encoding in (2a).
   (c) Explain why $m^{ed} \equiv m \pmod{n}$.
   (d) Encode the message "CAT" as an integer $m$, then find and compare $y \equiv m^{17} \pmod{2773}$ and $x \equiv y^{157} \pmod{2773}$. Explain why $x \neq m$.

(4) Creating your own key-pair:
   (a) Choose two large primes and compute $n = p \cdot q$ and $\phi(n)$.
   (b) Choose any $0 < e < \phi(n)$ in $\mathbb{Z}_n^\times$.
   (c) Write your $n$ and $e$ on the board; these make up your public key.
   (d) Find $d = e^{-1} \pmod{\phi(n)}$.

[1] Clifford Cocks, an English mathematician, had actually developed a version of this four years prior, but he didn't think it was worth publishing!

[2] For example, "DOG" becomes $041507 = 41507$.

[3] HINT: Try using the Chinese Remainder Theorem to work with smaller numbers.

(5) Sending messages[4]:
   (a) Find another group to exchange messages with. Come up with a message $m$ and encrypt it using that group's $n$ and $e$. Write your encrypted message on the board.
   (b) Once the other group has written their encrypted message for you on the board, decrypt it and see what they sent.
   (c) Pick any group's message on the board and see if you can decrypt it, using any techniques. What do you need to know before you can decrypt the message?

## FACTORING METHODS

(6) Factoring by **Trial Division**:
   (a) Let $n = 1643$ be the product of two primes. Factor $n$ by brute force, i.e., attempt to divide by each[5] prime up to $n$.
   (b) There is a $200,000 cash reward for factoring a 617-digit product of two primes. Explain why this is unreasonable to do by Trial Division.

> THEOREM: If $a^2 \equiv b^2 \pmod{n}$, then $\gcd(a+b,n)\cdot\gcd(a-b,n) = n$. Furthermore, if $a \not\equiv \pm b \pmod{n}$, then $\gcd(a+b,n)$ and $\gcd(a-b,n)$ are non-trivial factors of $n$.

(7) Factoring by the **Continued Fraction Algorithm**:
   (a) Let $n = 3053$ be the product of two primes. Find the **factor base** of $n$: the set of positive primes[6] $q_i \leq 7$ where $\left(\dfrac{n}{q_i}\right) = 1$.
   (b) Check[7] that each element in the factor base is not a prime factor of $n$.
   (c) Find the first[8] 5 convergents $C_k = \dfrac{p_k}{q_k}$ of $\sqrt{n}$. For each of these, compute $a_k \equiv p_k \pmod{n}$ and $b_k \equiv p_k^2 \pmod{n}$.
   (d) Write each $b_k$ as a product of primes in the factor base, if possible[9]. Find a nonempty set of pairs $(a_i, b_i), \ldots, (a_j, b_j)$ such that $b_i \cdots b_j$ is trivially a square modulo $n$ and
$$a_i \cdots a_j \not\equiv \pm\sqrt{b_i \cdots b_j} \pmod{n}$$
.
   (e) Let $A \equiv a_i \cdots a_j \pmod{n}$ and $B \equiv \sqrt{b_i \cdots b_j} \pmod{n}$. Calculate and compare $A^2 \pmod{n}$ and $B^2 \pmod{n}$.
   (f) Apply the Theorem, and use the Euclidean Algorithm to find the prime factors of $n$.

---

[4] If at any point you're waiting, work ahead on future problems!

[5] HINT: Start by determining a reasonable upper bound for the smallest prime factor of $n$, and then divide and conquer.

[6] The upper bound of 7 was not arbitrary; $7 = \lfloor e^{\frac{1}{2}\sqrt{\ln(n)\ln(\ln(n))}} \rfloor$.

[7] If an element were to be a factor of $n$, then we can reduce $n$ by that factor and try again.

[8] This choice was arbitrary. If we wish to do this in general, we'll take one convergent at a time until we find a solution.

[9] If $b_k$ isn't possible, try $-b_k = (-1)p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$.

# (Some) Primes between 1000 and 9999

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8539 | 5801 | 3251 | 7487 | 3083 | 8269 | 5749 | 4127 | 3823 | 1871 | 1567 | 1777 | 5711 |
| 7817 | 3529 | 2239 | 2797 | 6691 | 6247 | 2579 | 1307 | 2749 | 5813 | 6091 | 5651 | 1499 |
| 4337 | 7589 | 6143 | 8741 | 9283 | 1321 | 8011 | 2657 | 7043 | 8369 | 7219 | 2311 | 7681 |
| 8629 | 8039 | 1097 | 5021 | 7561 | 1237 | 2161 | 8849 | 9467 | 6571 | 2741 | 4549 | 4421 |
| 9533 | 9391 | 7793 | 9007 | 5849 | 9479 | 3643 | 6053 | 8171 | 9209 | 2069 | 2459 | 7193 |
| 7159 | 5501 | 7841 | 7573 | 9859 | 2647 | 6679 | 3163 | 7649 | 6173 | 5011 | 7541 | 1291 |
| 6277 | 1789 | 2609 | 8573 | 5303 | 5657 | 5179 | 9649 | 6131 | 1753 | 4597 | 5953 | 9551 |
| 8761 | 3881 | 3407 | 2699 | 4493 | 8677 | 4657 | 1481 | 4457 | 9629 | 8599 | 8147 | 7549 |
| 4591 | 9067 | 5479 | 4229 | 8819 | 6287 | 3637 | 5927 | 7247 | 1217 | 6421 | 8093 | 6427 |
| 1439 | 5557 | 7451 | 6529 | 6491 | 8287 | 5323 | 7753 | 9103 | 1033 | 1609 | 3187 | 3023 |
| 6911 | 1973 | 7457 | 7499 | 1913 | 8123 | 1901 | 5851 | 7879 | 2693 | 1259 | 1123 | 8467 |
| 8689 | 9161 | 6737 | 9239 | 2969 | 4729 | 6899 | 2131 | 7919 | 9419 | 3391 | 9511 | 2113 |
| 3931 | 2753 | 1487 | 9967 | 1367 | 7703 | 3079 | 1069 | 6121 | 4157 | 1549 | 6043 | 9371 |
| 9721 | 8821 | 9199 | 9491 | 1627 | 3607 | 4139 | 1427 | 1399 | 9187 | 7949 | 9397 | 6373 |
| 9203 | 2383 | 5861 | 6547 | 4651 | 8543 | 5189 | 5683 | 6833 | 1999 | 1453 | 5413 | 6823 |
| 5449 | 3709 | 6971 | 5669 | 6977 | 7591 | 1301 | 8753 | 6197 | 2269 | 8389 | 6367 | 7547 |
| 1153 | 8867 | 3793 | 2557 | 6151 | 8537 | 3181 | 9803 | 5807 | 3049 | 4751 | 9949 | 9403 |
| 8209 | 1733 | 1741 | 3923 | 7019 | 3119 | 4639 | 8647 | 5113 | 3697 | 2879 | 7907 | 5923 |
| 5233 | 3889 | 9781 | 4523 | 5023 | 7993 | 8087 | 9539 | 4793 | 2437 | 9839 | 8641 | 3329 |
| 1669 | 2251 | 4801 | 3659 | 4049 | 9767 | 1093 | 2617 | 5417 | 8191 | 4261 | 3581 | 3673 |
| 5903 | 4783 | 6983 | 7013 | 8713 | 9349 | 6079 | 6599 | 3037 | 7621 | 6857 | 9241 | 2777 |
| 7243 | 9973 | 7207 | 6959 | 1229 | 7351 | 5641 | 6569 | 7433 | 5387 | 9311 | 5527 | 9689 |
| 3121 | 2399 | 3547 | 1091 | 6553 | 1279 | 1721 | 2273 | 7607 | 8951 | 7529 | 6073 | 7727 |
| 7901 | 1759 | 2423 | 3539 | 4831 | 2333 | 3089 | 7321 | 7669 | 6163 | 4759 | 4691 | 4969 |
| 8513 | 9857 | 3911 | 1289 | 1201 | 3853 | 5843 | 5647 | 7109 | 3677 | 3217 | 4519 | 1277 |
| 3767 | 3833 | 7757 | 5689 | 1979 | 1483 | 8837 | 3313 | 9787 | 9337 | 3449 | 4663 | 5653 |
| 1879 | 8563 | 9437 | 2153 | 5779 | 2347 | 8923 | 5279 | 4211 | 8419 | 6067 | 5419 | 9227 |
| 1621 | 9011 | 9619 | 6709 | 4703 | 5167 | 8971 | 9041 | 4463 | 3671 | 5347 | 8803 | 8429 |
| 3727 | 8069 | 1543 | 3533 | 3739 | 7507 | 2591 | 1559 | 6761 | 8831 | 1447 | 4093 | 6961 |
| 3469 | 9473 | 7489 | 1787 | 3343 | 4363 | 7829 | 8317 | 4679 | 4051 | 6359 | 7349 | 4021 |
| 7309 | 8297 | 5879 | 2099 | 9059 | 6011 | 7537 | 6449 | 4243 | 9431 | 4909 | 9341 | 6829 |
| 7213 | 2417 | 1187 | 8719 | 6997 | 4153 | 7297 | 9377 | 9293 | 9631 | 6089 | 2441 | 4253 |
| 1423 | 1451 | 4111 | 9091 | 1723 | 5273 | 6217 | 1009 | 2917 | 2897 | 1303 | 9661 | 8293 |
| 2677 | 6133 | 1061 | 1213 | 7883 | 5003 | 7723 | 7517 | 7691 | 1571 | 5443 | 5581 | 7307 |
| 3613 | 8969 | 4973 | 8929 | 3323 | 1063 | 2137 | 2833 | 4273 | 3433 | 2857 | 4129 | 1373 |
| 5399 | 4957 | 2539 | 2287 | 3701 | 5981 | 2887 | 7027 | 4583 | 4231 | 1747 | 4567 | 2039 |
| 1019 | 1021 | 2521 | 3557 | 4007 | 9871 | 3299 | 1049 | 5039 | 9497 | 1163 | 2473 | 2927 |
| 4507 | 7477 | 9221 | 8053 | 8807 | 4219 | 8081 | 3221 | 7417 | 2711 | 3373 | 8623 | 3851 |
| 7717 | 3821 | 7577 | 2063 | 1231 | 4861 | 7393 | 8009 | 7699 | 5087 | 3389 | 6113 | 9181 |
| 7069 | 6221 | 6451 | 9109 | 7559 | 6703 | 4817 | 9851 | 2551 | 2341 | 4721 | 2861 | 3907 |
| 2203 | 4391 | 3011 | 8747 | 3623 | 7283 | 6871 | 3359 | 8311 | 9749 | 7411 | 2351 | 4951 |
| 3361 | 3919 | 2027 | 8219 | 6361 | 9613 | 4919 | 2281 | 5821 | 8443 | 6803 | 1429 | 6299 |
| 8839 | 4517 | 6661 | 2801 | 8447 | 5147 | 6397 | 5531 | 1867 | 5119 | 1583 | 3041 | 9739 |
| 1601 | 4649 | 6389 | 4073 | 7867 | 1693 | 6883 | 3541 | 8779 | 9043 | 8017 | 3467 | 2339 |
| 8461 | 5297 | 9343 | 2357 | 1531 | 6791 | 9929 | 3691 | 6733 | 8933 | 2971 | 9817 | 8273 |
| 4079 | 1129 | 8699 | 6203 | 1523 | 4673 | 6907 | 5869 | 2803 | 3229 | 2707 | 5659 | 7369 |
| 4483 | 8179 | 8893 | 6779 | 6563 | 8731 | 2659 | 3929 | 3559 | 3527 | 2687 | 3779 | 4877 |
| 9461 | 8861 | 4177 | 4003 | 1283 | 4733 | 1223 | 8291 | 7103 | 1667 | 7853 | 5227 | 4993 |