RSA Talk

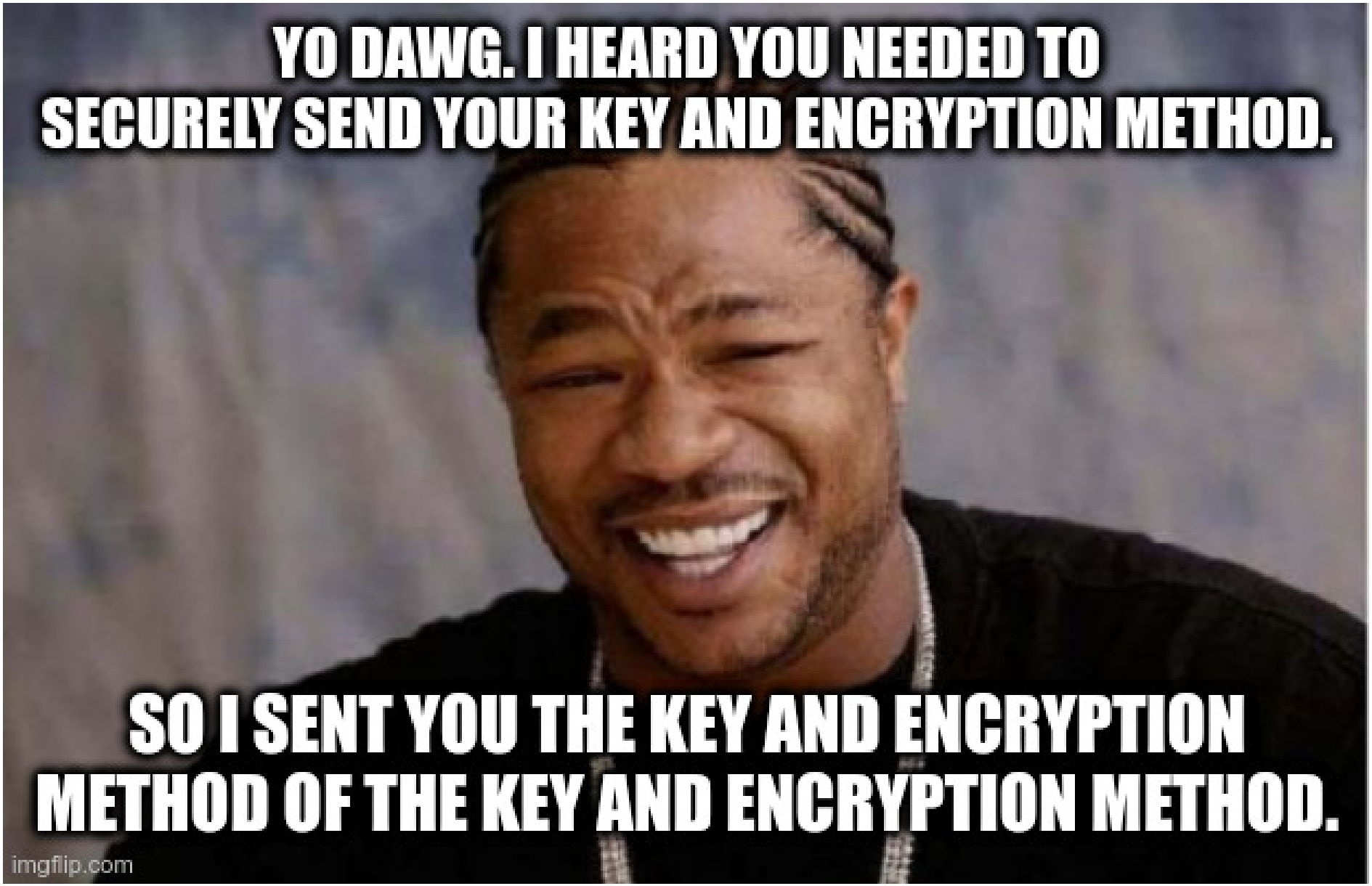
Eagle

August 17, 2023

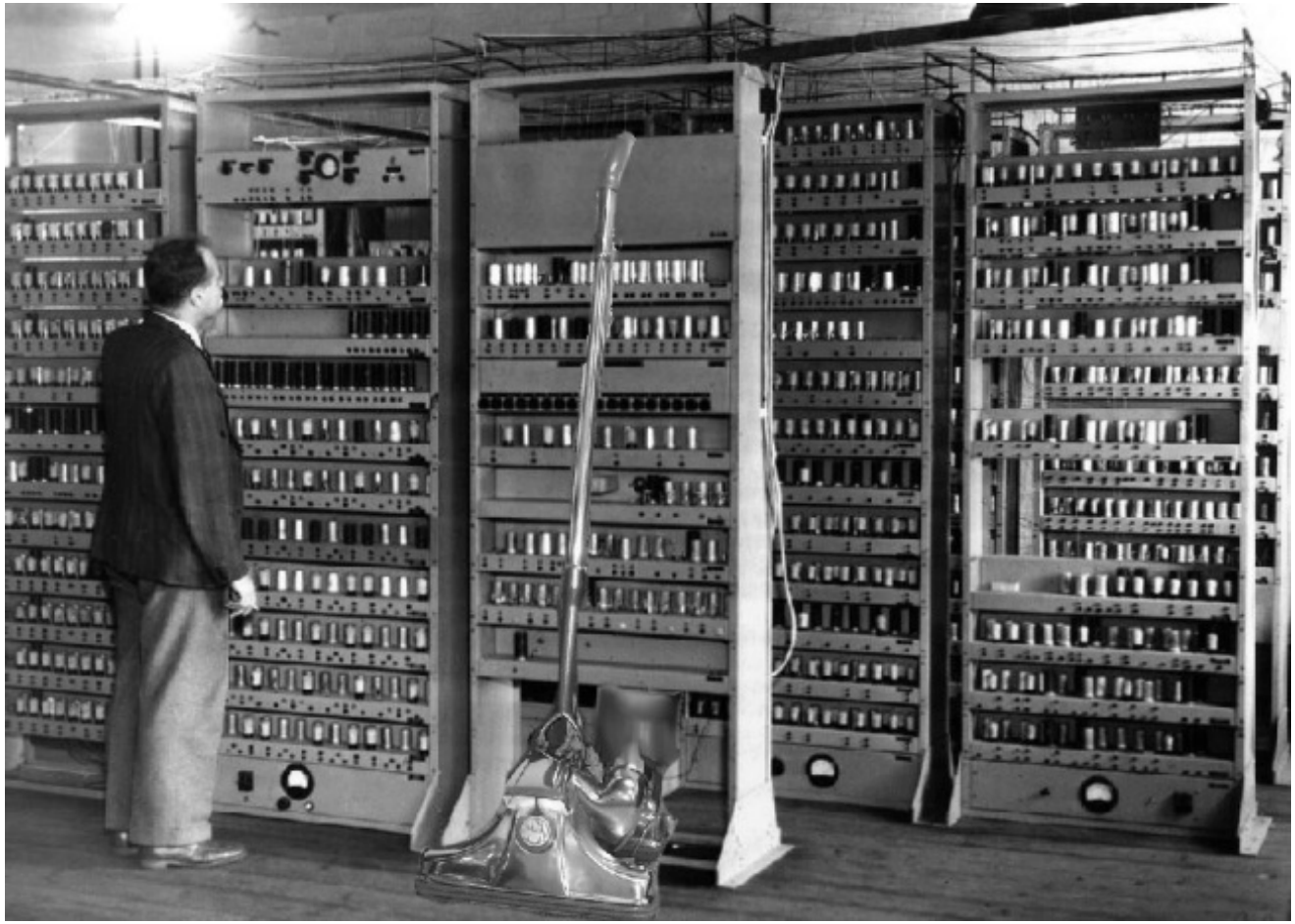
Agenda

1. Introduction
   - Cryptography
   - Brief History of RSA
   - Purpose of RSA
   - Relativity of RSA
2. RSA formulas
3. Modulus
4. Totients
5. Variables
6. Example
7. Vulnerabilities
   - Small Public Key
   - Small Private Key
   - Modulus

Cryptography Introduction



History of RSA



Fun Fact

RSA is an acronym of the creators' last names (Rivest–Shamir–Adleman).

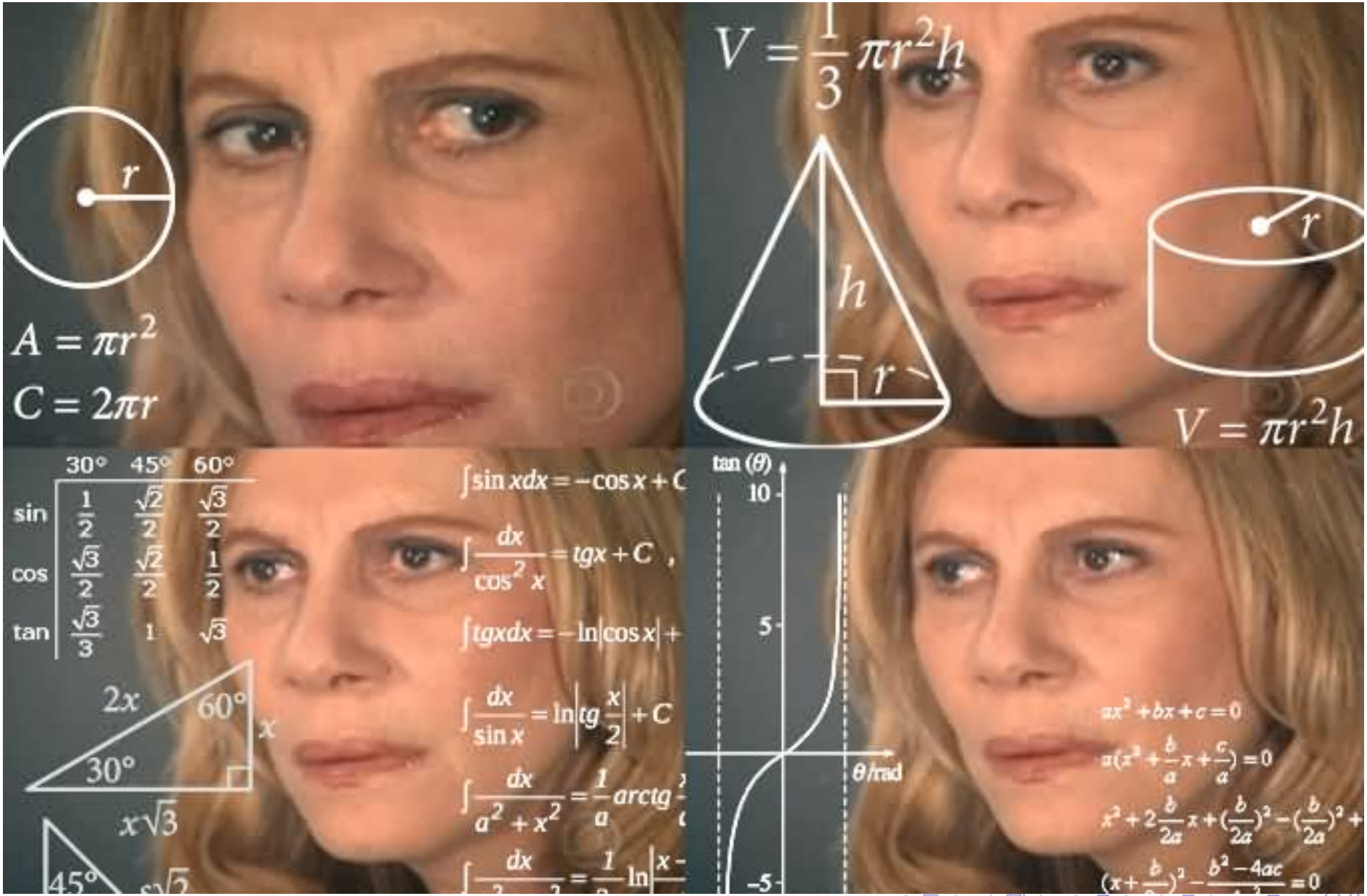
Purpose of RSA

RSA serves as a public key cryptography system that secures data over the internet. It is used in emails, ssl certificates, digital signatures, VPNs, communication, TLS handshakes, and so much more.

Important

RSA itself is secure when used correctly. We will be exploiting improper implementation by people who don't know how RSA works.

Relativity of RSA



Formulas

Main Formulas

$$C \equiv M^e \ mod \ n \tag{1}$$

$$M \equiv C^d \ mod \ n \tag{2}$$

$$de \equiv 1 \ mod \ \phi(n) \tag{3}$$

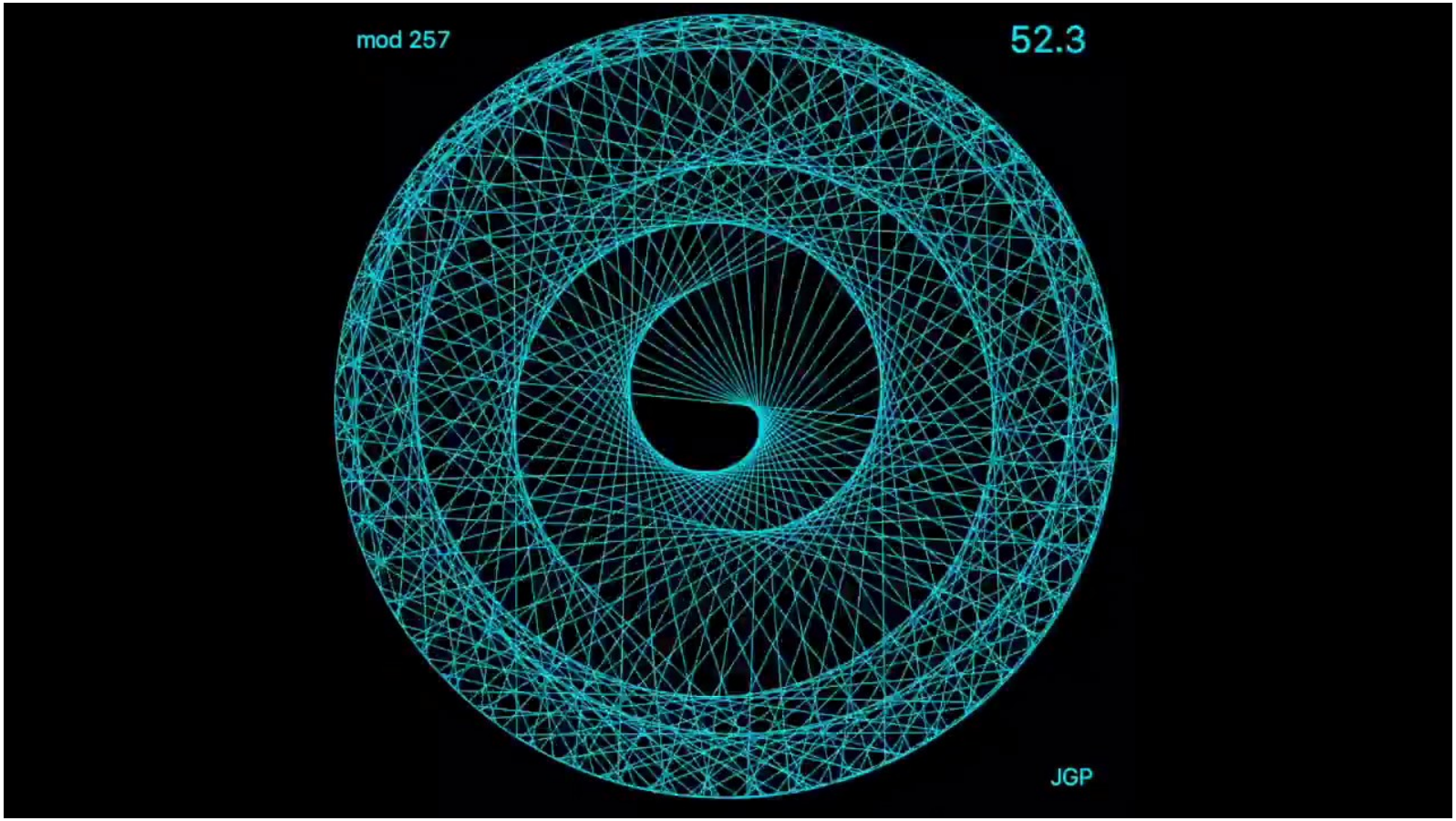
Additional Formulas

$$n = pq \tag{4}$$

$$\phi(n) = (p-1) \times (q-1) \tag{5}$$

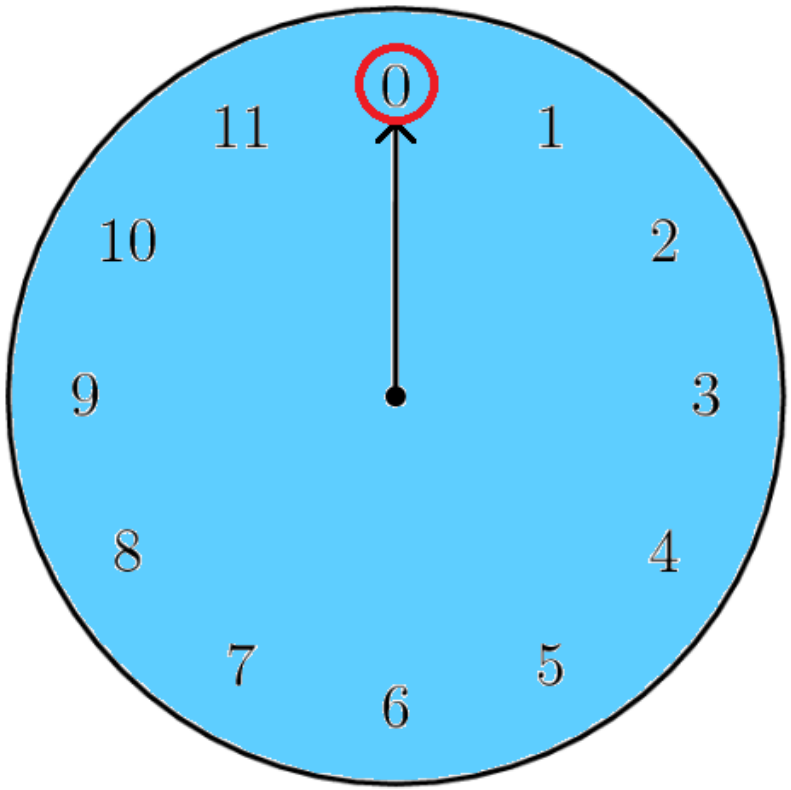
M = plaintext
C = ciphertext
e = public key exponent
d = private key exponent
n = modulus

Modular Arithmetic



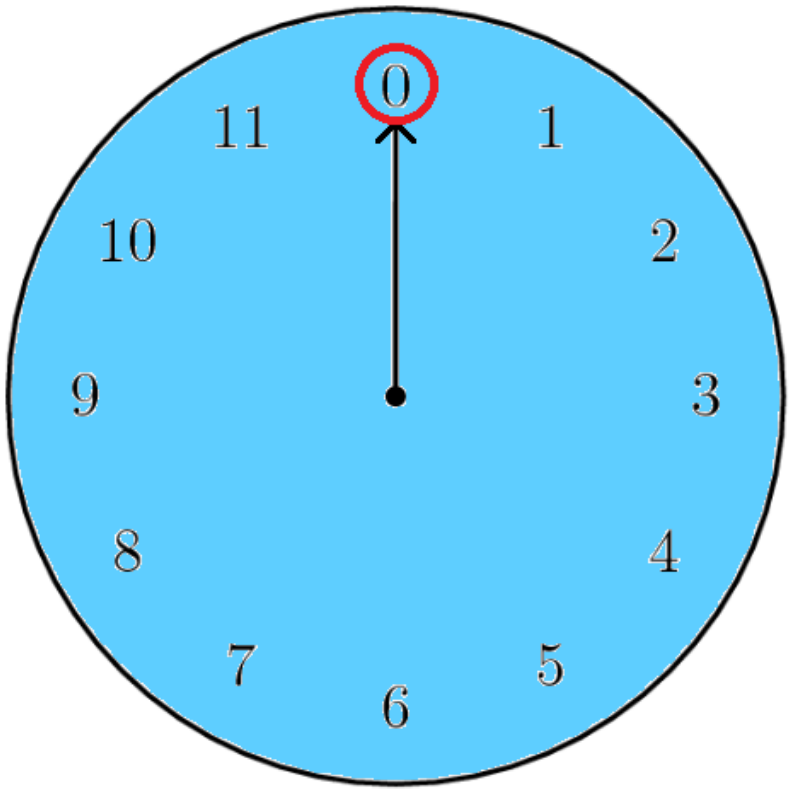
Modular arithmetic is a way of doing traditional operations with integers that "wrap around" when reaching a certain value.

Real World Use



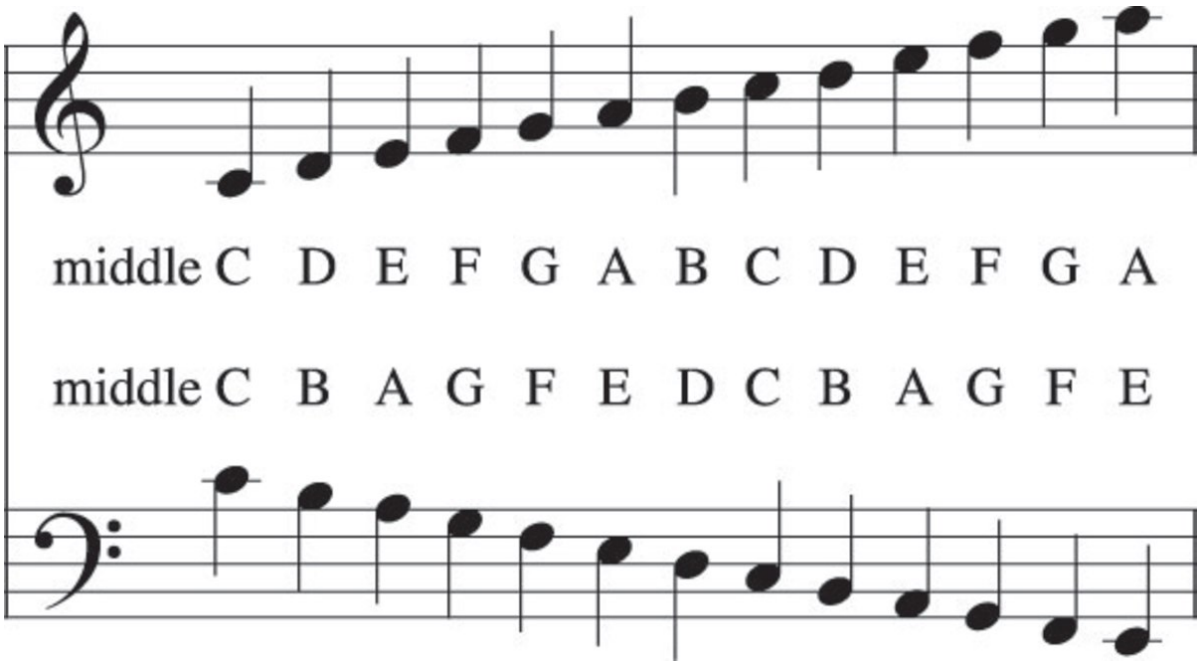
Example: If the time is 1:00, what will the time be in 30 hours?

Real World Use



Example: If the time is 1:00, what will the time be in 30 hours?
Answer: $x = (30 + 1) \mod 12 = (12 \times 2) + 7 \mod 12 = 7$.

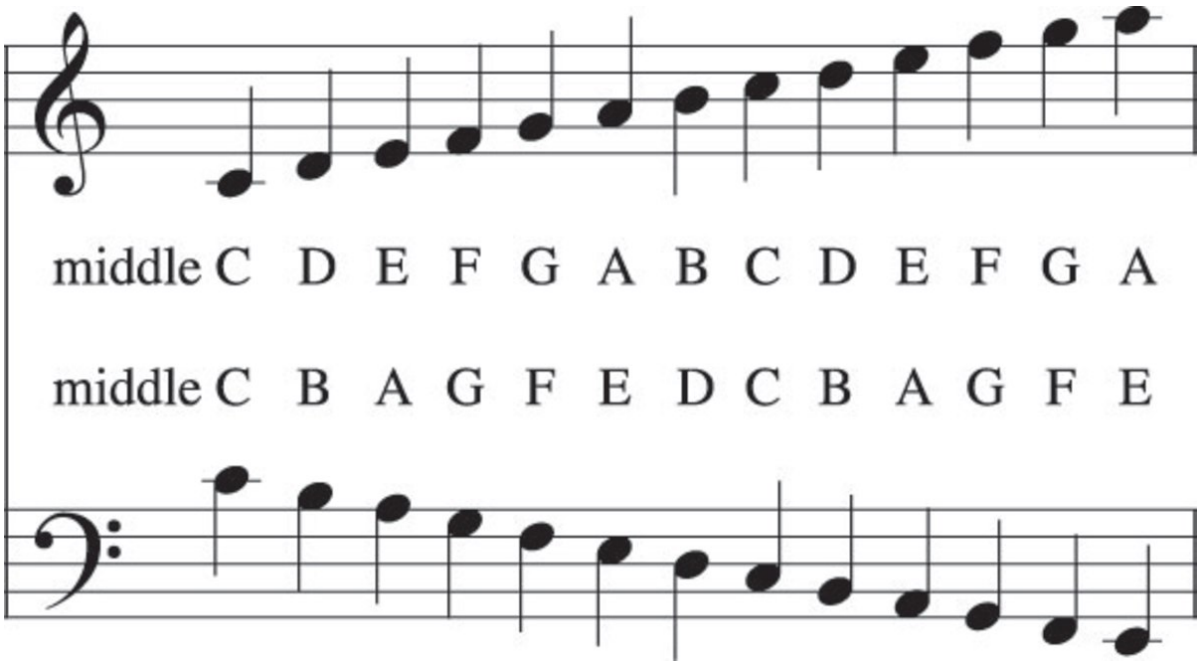
Real World Use



0	1	2	3	4	5	6
A	B	C	D	E	F	G

Example: If I am playing an F key at the bottom of a piano, what key am I playing 20 white keys away?

Real World Use



0	1	2	3	4	5	6
A	B	C	D	E	F	G

Example: If I am playing an F key at the bottom of a piano, what key am I playing 20 white keys away?

Answer: The modulus of a scale is 7 notes, and F corresponds to 5, so $x = (5 + 20) \mod 7 = (7 \times 3) + 4 \mod 7 = 4$ (E).

Congruent Modulo

Congruent modulo equation

$$a \equiv b \mod n \tag{6}$$

a and b are congruent modulo n if they share the same remainders when divided by n.
Example 1: $5 \equiv 15 \mod 10$ since the remainders of $15 \div 10$ and $5 \div 10$ are 5.

Congruent Modulo

Congruent modulo equation

$$a \equiv b \mod n \tag{6}$$

a and b are congruent modulo n if they share the same remainders when divided by n.

Example 1: $5 \equiv 15 \mod 10$ since the remainders of $15 \div 10$ and $5 \div 10$ are 5.

Example 2: $a \equiv 12 \mod 7$

Congruent Modulo

Congruent modulo equation

$$a \equiv b \mod n \tag{6}$$

a and b are congruent modulo n if they share the same remainders when divided by n.

Example 1: $5 \equiv 15 \mod 10$ since the remainders of $15 \div 10$ and $5 \div 10$ are 5.

Example 2: $a \equiv 12 \mod 7$

Answer: $a = 7 * x + 5$ with integer $x \geq 0$, e.g. 5, 12, 19, 26...

Congruent Modulo

Congruent modulo equation

$$a \equiv b \mod n \tag{6}$$

a and b are congruent modulo n if they share the same remainders when divided by n.

Example 1: $5 \equiv 15 \mod 10$ since the remainders of $15 \div 10$ and $5 \div 10$ are 5.

Example 2: $a \equiv 12 \mod 7$

Answer: $a = 7 * x + 5$ with integer $x \geq 0$, e.g. 5, 12, 19, 26...

Equivalency vs Equality

$\equiv$ is not $=$. In terms of modular arithmetic, $=$ represents the smallest solution to $\equiv$.

Bézout's identity [baizu]

Bézout's identity

$$ax + by = \gcd(a, b) \tag{7}$$

Example: $a = 12,\ b = 42$.
$\gcd(12, 42) = 6$: $12x + 42y = 6$.
One possible solution to Bézout's coefficients $(x, y) = (4, -1)$:
$(4)12 + (-1)42 = 6$.

Extended Euclidean Algorithm

Extended Euclidean Algorithm

$$ax + by = \gcd(a, b) \tag{8}$$

The **extended Euclidean algorithm** computes Bézout's coefficients.
Example: If $a = 140$ and $b = 3$, what are x and y?

Totients

Coprime means "relatively prime", as in prime to another number.
6 is not a prime number ($6 = 2 \times 3$), but it is **coprime** to 7 because $gcd(6, 7) = 1$.
Euler's totient ($\phi(n)$) is the number of coprime integers $< n$.
If p is prime:

Euler's Totient

$$\phi(p) = p - 1 \tag{9}$$

Example 1: $\phi(13) = 13 - 1 = 12$
Example 2: $\phi(2341) = ?$

Totients

Coprime means "relatively prime", as in prime to another number.
6 is not a prime number ($6 = 2 \times 3$), but it is **coprime** to 7 because $gcd(6, 7) = 1$.
Euler's totient ($\phi(n)$) is the number of coprime integers $< n$.
If p is prime:

Euler's Totient

$$\phi(p) = p - 1 \tag{9}$$

Example 1: $\phi(13) = 13 - 1 = 12$
Example 2: $\phi(2341) = ?$
Answer: $\phi(2341) = 2341 - 1 = 2340$.

Totients continued

If $n = pq$, where p and q are coprime:

Euler's Totient Multiplicative Property

$$\phi(n) = \phi(p) \times \phi(q) \tag{10}$$

Example 1: $\phi(77) = \phi(7) \times \phi(11)$ because $gcd(7, 11) = 1$. 7 and 11 are both prime numbers, so $\phi(77) = (7 - 1) \times (11 - 1) = 60$.

Example 2: $\phi(15) =?$

Totients continued

If $n = pq$, where p and q are coprime:

Euler's Totient Multiplicative Property

$$\phi(n) = \phi(p) \times \phi(q) \tag{10}$$

Example 1: $\phi(77) = \phi(7) \times \phi(11)$ because $gcd(7, 11) = 1$. 7 and 11 are both prime numbers, so $\phi(77) = (7 - 1) \times (11 - 1) = 60$.

Example 2: $\phi(15) =?$
$\phi(15) = (5 - 1) \times (3 - 1) = 8$

Euler's Totient

Euler's product formula

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p}) \tag{11}$$

Example 1: $\phi(20) = 5 \times 2^2$. Only count each prime once.
$\phi(20) = 20(1 - \frac{1}{5})(1 - \frac{1}{2} = 8)$.
Note: $\phi(20) \neq \phi(10) \times \phi(2)$ because 10 and 2 are not coprime.

Example 2: $\phi(568) =?$

Euler's Totient

Euler's product formula

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p}) \tag{11}$$

Example 1: $\phi(20) = 5 \times 2^2$. Only count each prime once.
$\phi(20) = 20(1 - \frac{1}{5})(1 - \frac{1}{2} = 8)$.
Note: $\phi(20) \neq \phi(10) \times \phi(2)$ because 10 and 2 are not coprime.

Example 2: $\phi(568) =?$
Answer: $\phi(568) = 71 \times 2^3$, both coprime ($gcd(2, 71) = 1$).
$\phi(568) = 568(1 - \frac{1}{71})(1 - \frac{1}{2}) = 280$.

Modulus

Modulus Formula

$$n = pq \tag{12}$$

Modulus Totient

$$\phi(n) = (p-1)(q-1) \tag{13}$$

n symbolizes the modulus in the RSA algorithm.

Because $n = pq$, $\phi(n) = \phi(p) \times \phi(q) = (p-1)(q-1)$.
Example: If $p = 59$ and $q = 23$, $n = 59 \times 23 = 1357$ and $\phi(n) = (59-1)(23-1) = 1276$.

Private and Public Keys

Key Generation

$$de \equiv 1 \mod \phi(n) \tag{14}$$

d and **e** symbolize the private and public key in the RSA algorithm.

e is coprime with $\phi(n)$ and $1 < e < \phi(n)$.
d is the modular multiplicative inverse of e.

Bézout's identity in modular inverse

Modular inverse

$$d \equiv e^{-1} \mod \phi(n) \tag{15}$$

Bézout's identity

$$ax + by = \gcd(a, b) \tag{16}$$

e and $\phi(n)$ are coprime: $gcd(e, n) = 1$.

$d \equiv e^{-1} \mod \phi(n)$

$de \equiv 1 \mod \phi(n)$

$de - 1 \equiv 0 \mod \phi(n)$

$k\phi(n) \equiv 0 \mod \phi(n)$

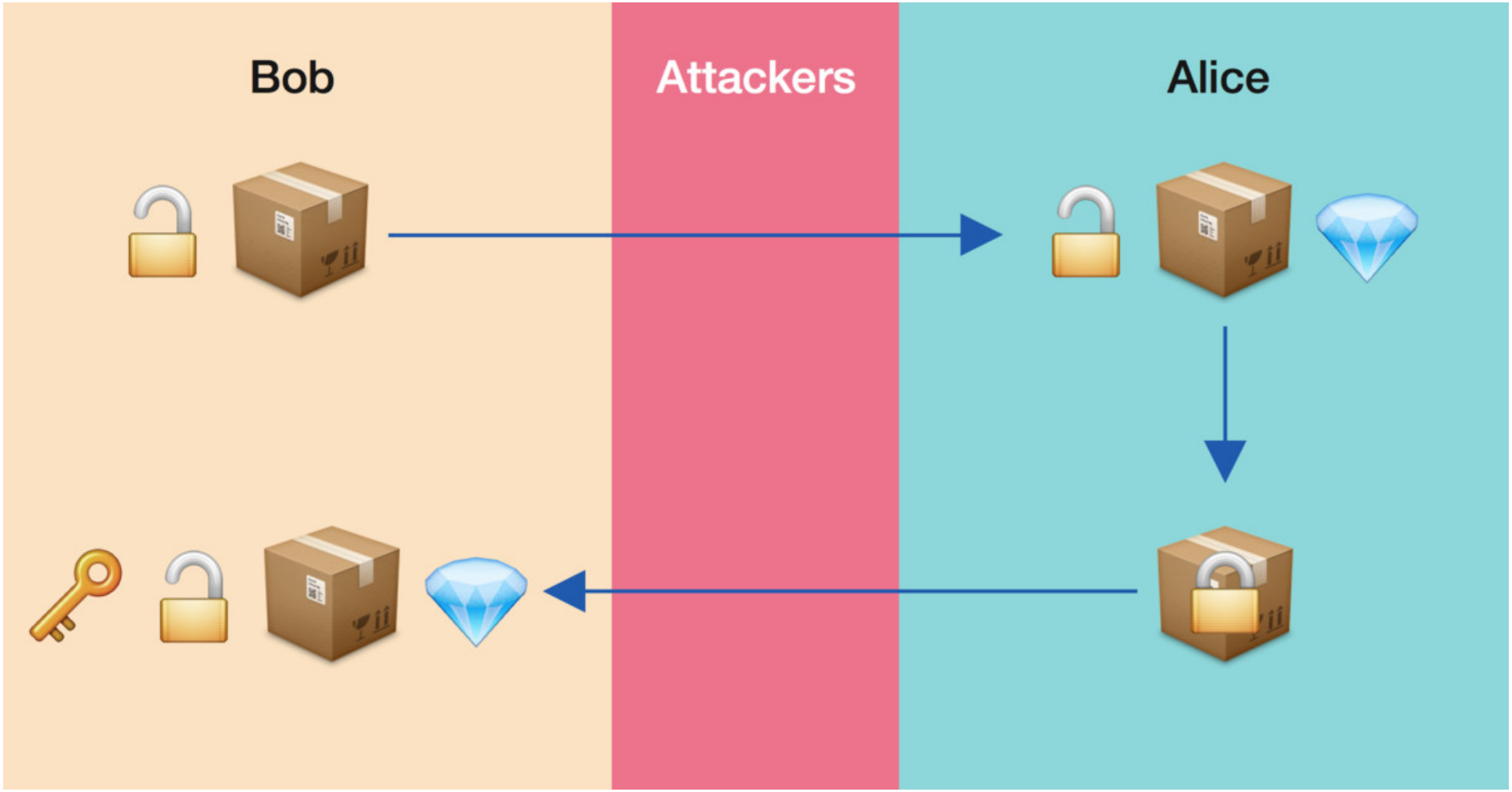
$de - 1 \equiv k\phi(n)$

$de - 1 - k\phi(n) \equiv 0$

$de - k\phi(n) \equiv 1$

The extended Euclidean algorithm finds Bézout's coefficients (d, k).

Background



Qualitative Example

1. Alice generates two primes p and q.
2. Alice multiplies two factors p and q to create modulus n.
3. Alice solves $(p-1)(q-1)$ to generate the modulus totient $\phi(n)$.
4. Alice generates public exponent e so $1 < e < \phi(n)$ and coprime to $\phi(n)$.
5. Alice generates private exponent d so $d \equiv e^{-1} \mod \phi(n)$.
6. Alice sends n and e to Bob.
7. Bob generates plaintext m where $m < n$.
8. Bob computes ciphertext C by using plaintext m in $C \equiv m^e \mod n$.
9. Bob sends ciphertext C to Alice.
10. Alice decrypts ciphertext C by solving $m \equiv C^d \mod n$.

Real CTF examples

To solidify understanding of how RSA is meant to work, here are two examples of real CTF challenges.

Examples: rsa-pop-quiz, Relatively-Secure-Algorithm

Vulnerabilities

Small e

A challenge may set $e = 1$.
$C \equiv m^e \mod n$ becomes $C = m \mod n$, and because $m < n$, $C = m$.

Example: Salty

Fun Fact

e is most commonly 3, 17, and 65537 because all are prime and Fermat numbers ($F_n = 2^{2^n} + 1$).
65537 (F_4) is the largest Fermat prime discovered.
F_{11} is the largest Fermat number completely factored at 617 digits.

Small e and m

If $m^e < n$, the message has not "looped around" the modulus.
$C = m^e \mod n = m^e$, so $C^{1/e} = m$.

Example: mini-rsa, Modulus-Inutilis

Wiener's Attack

Wiener's attack relies on a small private exponent d to expose itself.

Wiener's Theorem

$$d < \frac{1}{3} N^{\frac{1}{4}} \tag{17}$$

$de \equiv 1 \mod \phi(n)$
$de = k\phi(n) + 1$
Divide by dn: $\frac{e}{n} = \frac{k}{d} * \frac{\phi(n)}{n} + \frac{1}{d*n}$.
$\frac{1}{d*n} \approx 0$: $\frac{e}{n} \approx \frac{k}{d} * \frac{\phi(n)}{n}$
$\frac{e}{n} * \frac{d}{k} \approx \frac{\phi(n)}{n}$
Find the convergents of the continued fraction expansion of $\frac{e}{n}$.

Example: dachshund, b00tl3gRSA2, sosig

Too many primes

When $n = pqrst\ldots$, it becomes easier to factor n.

Examples: b00tl3gRSA3, Manyprime

One prime

Because n is a product of two primes, $\phi(n) = (p-1)(q-1)$. However, n as a prime would make $\phi(n) = (n-1)$.

Example: Monoprime

Same primes

Instead of $n = pq$, $n = p^2$: $\sqrt{n} = p$. Therefore, $\phi(n) = n(1 - \frac{1}{p})$

Euler's totient of a prime power argument

If p is prime and $k \geq 1$:

$$\phi(p^k) = p^k(1 - \frac{1}{p})$$

Example: square-eyes

Conclusion

Any questions?

RSA Talk

Eagle

August 17, 2023