Prime Number Generation

Prime Numbers

- ★ Prime Numbers: Has exactly two divisors.
- ★ If 'N' is prime, then the divisors are 1 and N.
- ★ All numbers have prime factors.

Numbers	10	11	100	37	308	14688
Prime Factorization	$2^1 \times 5^1$	$1^1 \times 11^1$	$2^2 \times 5^2$	$1^1 \times 37^1$	$2^2 \times 7^1 \times 11^1$	$2^5 \times 3^3 \times 17^1$
Prime Numbers	2, 5	1, 11	2, 5	1, 37	2, 7, 11	2, 3, 17

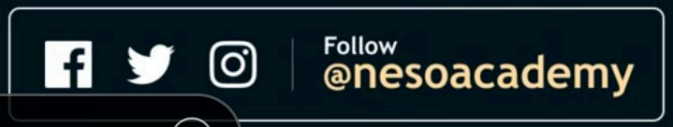
Prime Numbers

- ★ Prime Numbers: Has exactly two divisors.
- ★ If 'N' is prime, then the divisors are 1 and N.
- ★ All numbers have prime factors.

Numbers	10	11	100	37	308	14688
Prime Factorization	$2^1 \times 5^1$	$1^1 \times 11^1$	$2^2 \times 5^2$	$1^1 \times 37^1$	$2^2 \times 7^1 \times 11^1$	$2^5 \times 3^3 \times 17^1$
Prime Numbers	2, 5	1, 11	2, 5	1, 37	2, 7, 11	2, 3, 17

Prime Numbers – Example

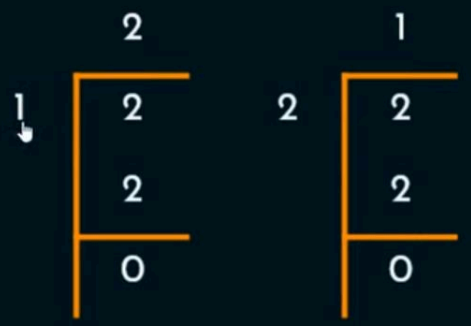
- ★ 2 is a prime number.
- ★ 3 is a prime number.
- ★ 5 is a prime number.
- ★ 7 is a prime number.
- ★ 9 is not a prime number.
- ★ 9 is a composite number.



View key concept

Prime Numbers – Example

- ★ 2 is a prime number.
- ★ 3 is a prime number.
- ★ 5 is a prime number.
- ★ 7 is a prime number.
- ★ 9 is not a prime number.
- ★ 9 is a composite number.
- ★ 33 is a composite number.



Prime Numbers – Example

- ★ 2 is a prime number.
- ★ 3 is a prime number.
- ★ 5 is a prime number.
- ★ 7 is a prime number.
- ★ 9 is not a prime number.
- ★ 9 is a composite number.
- ★ 33 is a composite number.

Divisors of 33: 1, 3, 11 and 33

Facts about primes

- ★ Only even prime : 2
- ★ Smallest prime number : 2
- ★ Is 1 a prime number? No.
- ★ Except for 2 and 5, all prime numbers end in the digit 1, 3, 7 or 9.

Why prime numbers in cryptography?

- ★ Many encryption algorithms are based on prime numbers.
- ★ Very fast to multiply two large prime numbers.
- ★ Extremely computer-intensive to do the reverse.
- ★ Factoring very large prime numbers is very hard i.e. take computers a long time.

Random Number Generation

Pseudorandom Number Generator

Pseudorandom Number Generator

- ★ Stream cipher.
- ★ Key stream generator.
- ★ Truly random sequence.

Pseudorandom Number Generator

PTS	X_1	X_2	X_3	X_4	.	.	.	.	X_n
⊕ KS	K_1	K_2	K_3	K_4	.	.	.	.	K_n
CTS	Y_1	Y_2	Y_3	Y_4	.	.	.	.	Y_n

Alice

Bob

CTS	Y_1	Y_2	Y_3	Y_4	.	.	.	.	Y_n
⊕ KS	K_1	K_2	K_3	K_4	.	.	.	.	K_n
PTS	X_1	X_2	X_3	X_4	.	.	.	.	X_n

Pseudorandom Number Generator

- ★ Plaintext : X_i
- ★ Key Stream : K_i
- ★ Ciphertext : Y_i

Encryption (Y_i) : $X_i \oplus K_i$

Decryption (X_i) : $Y_i \oplus K_i$

K_i is a truly randon bit.

This stream cipher is referred to as One Time Pad (Perfect Secrecy).

Pseudorandom Number Generator

- ★ Stream cipher.
- ★ Key stream generator.
- ★ Truly random sequence.
- ★ P(0) = P(1).
- ★ Shannon notion of perfect secrecy.
- ★ Generating truly random sequence is impractical.
- ★ Pseudorandom sequence.
- ★ A good stream cipher – close to truly random sequence.
- ★ Randomness.
- ★ How to measure the randomness?
- ★ Randomness is inevitable.