12 ශ්‍රේණිය තොරතුරු හා සන්නිවේදන තාක්ෂණය 9 වන සතිය - ජූනි 29 සිට ජූලි 3 දක්වා

නිපුණතා මට්ටම 11.1 - අන්තර්ජාලයට සම්බන්ධ කර ඇති උපාංගවල ආරක්ෂණය සහ සන්නිවේදනයේ ඇති ආරක්ෂක ආකාර විමර්ශනය කරයි.

දත්ත කේතනය - අන්තර්ජාලය ඔස්සේ පාර්ශ්ව අතර සම්ප්‍රේෂණය වන දත්තවල රහස්‍යභාවය සුරැකීම සඳහා භාවිත කරන ගුප්ත (cryptography) කේතන ක්‍රමවේදයකි.

දත්ත කේතනය සිදු කරන ආකාර දෙකකි.

සම්මිතික යතුරු කේතනය (Symmetric Key Encryption)

මෙහිදී දත්ත කේතනයට සහ විකේතනයට භාවිත කරන්නේ එකම යතුරකි.මෙහිදී දත්ත සම්ප්‍රේෂණය සිදු කිරීමට පෙර සන්නිවේදන පාර්ශ්ව විසින් දත්ත කේතනය/විකේතනය සඳහා භාවිත කරන යතුර ලබා ගත යුතුය.

අසම්මිතික යතුරු කේතනය (Asymmetric Key Encryption)

මෙම ක්‍රමවේදයේදී දත්ත කේතනයට සහ විකේනයට එකිනෙක වෙනස් යතුරු දෙකක් භාවිත කෙරේ.දත්ත සම්ප්‍රේෂණයේදී ඊට හවුල් වන සියලුම සන්නිවේදන පාර්ශ්වවලට එකිනෙකට වෙනස් යතුරු යුගලයක් තිබීම අත්‍යවශ්‍ය වේ.එම යතුරු යුගලය පෞද්ගලික යතුර සහ පොදු යතුර ලෙස හඳුන්වයි.කේතනය කළ කිසියම් දත්තයක් විකේතනය කළ යුතු නම්,කේතනය කිරීමට භාවිත කළ යතුර සහ විකේතනයට භාවිත කරන යතුර ගණිතමය වශයෙන් ගැළපිය යුතුය.මෙම ක්‍රමය මගින් සාර්ථකව විකේතනය වුවහොත් කේතාංකය නැවතත් කියවිය හැකි පෙළක් බවට පත් විය යුතුය.

අභ්‍යාස

1.අංකිත අත්සන යන්න හඳුන්වා එහි වැදගත්කම පහදන්න.

2.ජාලගත පද්ධති විසින් මුහුණ දෙනු ලබන විවිධ තර්ජන මොනවාද?

3.බල නොලත් සහ හානිකර ප්‍රවේශවීම්වලින් ආරක්ෂා වන්නේ කෙසේද?