EFF'S SURVEILLANCE SELF-DEFENSE

အစ-အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းအား ထဲထဲဝင်ဝင်လေ့လာခြင်း- အများသုံး စကားဝှက်သော့ဖြင့် ကုဒ်ပြောင်းလဲခြင်း စနစ်တွေ ဘယ်လို အလုပ်လုပ်သလဲ။

---

https://ssd.eff.org/en/about-surveillance-self-defense

LOCALIZATION LAB

အစ-အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းအား ထဲထဲဝင်ဝင်လေ့လာခြင်း- အများသုံး စကားဝှက်သော့ဖြင့် ကုဒ်ပြောင်းလဲခြင်းစနစ်တွေ ဘယ်လို အလုပ်လုပ်သလဲ။

နောက်ဆုံးစိစစ်သည့်ရက်စွဲ ၀၁-၀၆-၂၀၂၁

အစ-အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်း end-to-end encryption စနစ်ကို မှန်ကန်စွာအသုံးပြုမယ်ဆိုရင် သင့်မက်ဆေ့ချ်တွေ၊ စာတွေနဲ့ဖိုင်တွေကို လက်ခံသူကလွဲလို့ အခြားသူတွေဖတ်မရ/သုံးမရအောင် လုပ်ပြီး သင့် ဒေတာတွေကို အကာအကွယ်ပေးနိုင်ပါတယ်။ အဲ့ဒီစနစ်ကို နောက်တနေရာမှာသုံးလို့ရပါသေးတယ်။ ပို့လိုက်တဲ့သူဆီက မက်ဆေ့ချ်ကို ကြားဖြတ် ပြုပြင်ပြောင်းလဲထားခြင်းရှိ/မရှိကိုပါ အတည်ပြု စစ်ဆေးတဲ့နေရာမှာ သုံးလို့ရပါတယ်။

လွန်ခဲ့တဲ့နှစ်အနည်းငယ်ကစလို့ အစ-အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်း tools တွေက ပိုပြီး အသုံးဝင်လာပါတယ်။ အစ-အဆုံး ကုဒ်ဖြင့်ပြောင်းလဲခြင်းဆိုတဲ့ ပေးပို့သူနဲ့ လက်ခံသူအကြား မက်ဆေ့ချ်တွေကို ကုဒ်ဖြင့်ပြောင်းလဲခြင်း encrypt ကို အသုံးပြုတဲ့ အက်ပလီကေးရှင်းတွေနဲ့ ပတ်သက်လို့ ဥပမာကောင်းပြရရင် iOS ရော Android မှာပါသုံးလို့ရတဲ့ Signal လိုမျိုး စကားပြောခေါ်ဆိုမှု၊ ဗီဒီယို ခေါ်ဆိုမှု၊ ချက်တင်နဲ့ ဖိုင်အပေးအယူတွေကို လုံခြုံစိတ်ချစွာ မက်ဆေ့ချ်ပို့လို့ရတဲ့ နည်းစနစ် Secure messaging tools သုံး အက်ပ်တွေပါပဲ။ ဒီနည်းစနစ်တွေက နက်ဝေါ့ခ်ထဲမှာ စောင့်ကြည့်ထောက်လှမ်း သူတွေ (သို့မဟုတ်) ဝန်ဆောင်မှုပေးသူတွေကိုယ်တိုင် မက်ဆေ့ချ်တွေကို ဖတ်မရအောင် လုပ်ထားပေး ပါတယ်။

ဒါပေမဲ့ အချို့ အစ-အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းနည်းလမ်းတွေကို နားလည်ဖို့နဲ့ အသုံးပြုဖို့ အခက်အခဲ တွေရှိနေပါတယ်။ အစ-အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို အသုံးမပြုခင်မှာ အများသုံးစကားဝှက်သော့ပါ ဝှက်စာ ဗေဒ public key cryptography ရဲ့ အခြေခံကိုအချိန်ယူပြီး နားလည်အောင် အရင်လုပ် သင့်ပါတယ်။

ဤလမ်းညွှန်တွင် ကျွန်ုပ်တို့ပြောနေသော ကုဒ်ဖြင့်ပြောင်းလဲခြင်း အမျိုးအစားမှာ အစ-အဆုံးကုဒ်ဖြင့် ပြောင်းလဲခြင်းနည်းလမ်းတွေကို မှီခိုအားထားခြင်းကြောင့် အများသုံး စကားဝှက်သော့ပါ ဝှက်စာဗေဒ

public key cryptography သို့မဟုတ် အများသုံးစကားဝှက်သော့ပါ ကုဒ်ဖြင့်ပြောင်းလဲခြင်း public key encryption ဟုခေါ်သည်။ အခြား ကုဒ်ဖြင့်ပြောင်းလဲခြင်း အမျိုးအစားများအကြောင်းကို ဖတ်ရန် ကျွန်ုပ်တို့ရဲ့ What Should I Know About Encryption? ဆိုတဲ့ လမ်းညွှန်ကိုလည်း ကြည့်ရှု နိုင်ပါတယ်။

အများသုံးစကားဝှက်သော့ပါ ဝှက်စာဗေဒ ရဲ့ အခြေခံမူတွေကို နားလည်ထားခြင်းက ဒီနည်းပညာကို အောင်အောင်မြင်မြင်သုံးနိုင်ဖို့ အထောက်အကူပြုပါလိမ့်မယ်။ အများသုံးစကားဝှက်သော့ပါ ဝှက်စာဗေဒ ကိုသုံးပြီး ကိုယ်လုပ်နိုင်တာတွေနဲ့ မလုပ်နိုင်တာတွေကိုသိမှ ဘယ်နေရာမှသုံးရမလဲဆိုတာကို ဆုံးဖြတ်နိုင်မှာပါ။

ကုဒ်ဖြင့်ပြောင်းလဲခြင်းက ဘာတွေလုပ်ပေးနိုင်သလဲ။

သင်မက်ဆေ့ချ်တစ်ခုကို ပို့လိုက်တဲ့အခါ ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို ဒီလိုလုပ်ပါတယ်။

(၁) “hello mum (ဟဲလို၊ အမေ)” ဆိုတဲ့ ရှင်းရှင်းလင်းဖတ်လို့ရတဲ့ မက်ဆေ့ချ်ကို ဖတ်မရတဲ့ “OhsieW5ge+osh1aehah6” စာစုဖြစ်အောင် ပြောင်းလဲလိုက်ပါတယ်။

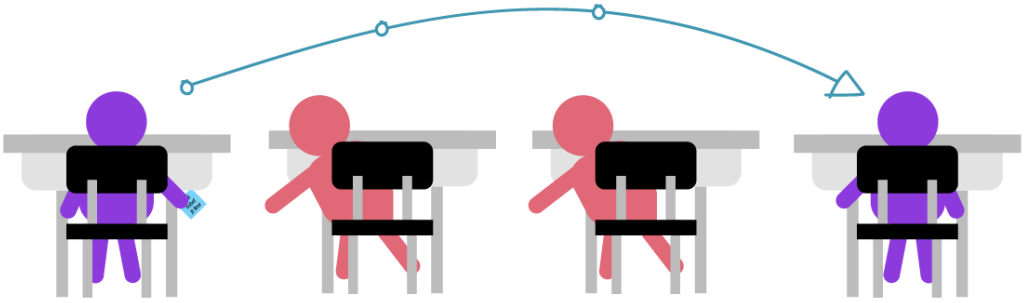
(၂) ဒီ ဖတ်မရတဲ့ ကုဒ်နဲ့ပြောင်းလဲထားတဲ့စာစု“OhsieW5ge+osh1aehah6” ကို အင်တာနက်တလျှောက်ပေးပို့လိုက်ပါတယ်။

(၃) အဲဒီစာစုက လက်ခံသူဆီရောက်သွားတဲ့အခါမှာတော့ ပြန်ဖြည်လိုက်ပြီး မူလစာစု ဖြစ်တဲ့ “hello mum (ဟဲလို၊ အမေ)” လို့ပြန်မြင်ရမှာဖြစ်ပါတယ်။

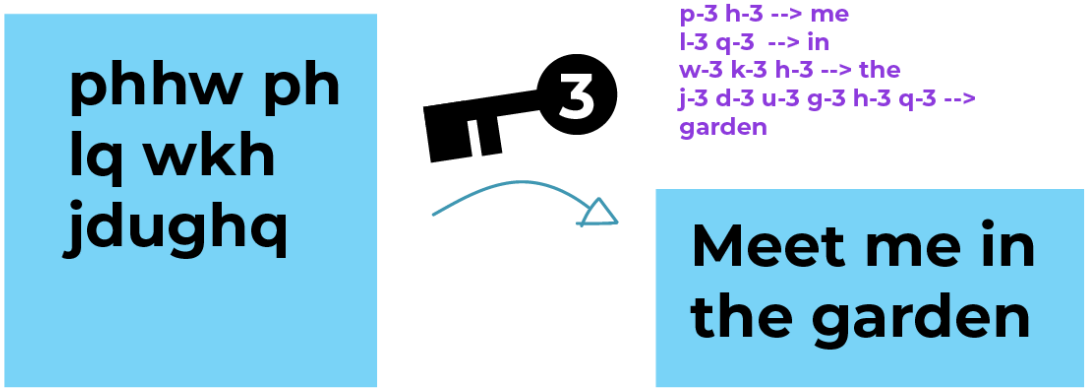
ဘက်ညီသောကုဒ်ဖြင့်ပြောင်းလဲခြင်း - စကားဝှက်သော့ တစ်ချောင်းတည်း အသုံးပြုပြီး လျှို့ဝှက်စာများပေးပို့ခြင်းပုံပြင်

ဇာတ်လမ်းအစမှာ ဂျူလီယာက ဆီဇာဆီ စာတစ်စောင်ပို့လိုက်တယ်။ စာထဲမှာ “ပန်းခြံမှာဆုံရအောင်” လို့ရေးထားတယ်။ ဒါပေမဲ့ အဲ့ဒီစာကို သူမရဲ့ အတန်းဖော်တွေ မမြင်သွားစေချင်ဘူး။

ဆီဇာ့ဆီကို စာရောက်ဖို့ သူငယ်ချင်းတွေကတဆင့် စာကိုပို့ရမှာပါ။ စာပို့ပေးသူတွေအားလုံးက သူတို့ နှစ်ယောက်နဲ့ပတ်သက်လို့ ဘာမှမဖြစ်ပေမဲ့ စာကိုခိုးဖတ်ပြီး ဟောင်ဖွာဟောင်ဖွာလုပ်မဲ့သူတွေဖြစ်နေတယ်။ ဒါ့အပြင်ဆီဇာ့ဆီမရောက်ခင် စာကို မိတ္တူတွေလည်းပွားထားဦးမှာဖြစ်တယ်။



ဒါ့ကြောင့် ပို့မယ့်မက်ဆေ့ချ်ကို encrypt ကုဒ်နဲ့ပြောင်းလဲတဲ့နည်းလမ်းတစ်ခုဖြစ်တဲ့ သုံးလုံးမြောက် အက္ခရာနဲ့အစားထိုးတဲ့သော့ကုဒ်နဲ့ ဝှက်စာရေးဖို့ ဂျူလီယာကဆုံးဖြတ် လိုက်တယ်။ အဲဒီနည်းလမ်းမှာ အက္ခရာတစ်ခုကို သူ့ရဲ့နောက် ၃ လုံးမြောက်က အက္ခရာတစ်ခုနဲ့အစားထိုးတဲ့နည်းလမ်းကိုသုံးတဲ့အတွက် A နေရာမှာ D၊ B နေရာမှာ E စသဖြင့် အစားထိုးသွားတာပါ။ ဆိုလိုတာက ဂျူလီယာနဲ့ဆီဇာက ကုဒ်နဲ့ပြောင်းလဲဖို့ရော၊ ပြန်ဖြည်ဖို့ရောအတွက် သုံးလုံး မြောက်အက္ခရာနဲ့အစားထိုးတဲ့ သော့ကုဒ်ကို သုံးထားတဲ့အတွက် ပြန်ဖြည်ဖို့ လွယ်ပါတယ်။ ဒီနည်းလမ်းက ဖြစ်နိုင်ချေကုဒ်တွေအားလုံးကို တွက်ချက်ပြီး ကုဒ်လိုက်ဖြည်တဲ့ တိုက်ခိုက်မှု ဖြစ်တဲ့ “brute force” ကို သုံးလိုက်ရင် ကုဒ်ပွင့်သွားဖို့ လွယ်ပါတယ်။ ဆိုလိုတာက ပြန်ဖြည်တဲ့ကုဒ်ကို အဖြေရတဲ့အထိ ခန့်မှန်းတွက်ချက်ပြီး လိုက်ထည့်လို့ရ တယ်ဆိုတာပါပဲ။



ဒီလိုအကွာရာတစ်ခုကို သူ့ရဲ့နောက်သုံးလုံးမြောက်နဲ့အစားထိုးရေးတဲ့ ဝှက်စာရေးနည်းက ဂျူးလီးယက်ဆီဇာအသုံးပြုခဲ့တဲ့ သမိုင်းဝင်ဥပမာတစ်ခုဖြစ်ပါတယ်။ ဆီဇာဝှက်စာပုံသေနည်း လို့ခေါ်ပါတယ်။ ဝှက်စာပြောင်းဖို့ ရော၊ ပြန်ဖြည်ဖို့ရောအတွက် စကားဝှက်သော့တစ်ခုပဲလိုပါတယ်။ ဒီဥပမာမှာဆိုရင် စာလုံး(၃) လုံးမြောက်ပေါ့။ အဲဒီလိုဝှက်စာပြောင်းဖို့ ရော၊ ပြန်ဖြည်ဖို့ရောအတွက် စကားဝှက်သော့တစ်ခုပဲသုံးတဲ့နည်းလမ်းကို ဘက်ညီဝှက်စာ ဗေဒ cryptography လို့ခေါ်ပါတယ်။

ဆီဇာဝှက်စာက ဘက်ညီဝှက်စာထဲမှာ ပြန်ဖြည်ရလွယ်ကူတဲ့ အမျိုးအစားထဲပါဝင်ပါတယ်။ ကံကောင်းတာက ဆီဇာ ဝှက်စာကနေ အဆင့်ဆင့်ပြောင်းလဲခဲ့တာ အခုဆိုရင်တော့ ပြန်ဖြည်ရအလွန်ခက်တဲ့ဝှက် စာတွေရေးနိုင်တဲ့ကုဒ်တွေကိုသုံးနိုင်တဲ့ အဆင့်ကို ရောက်နေပါပြီ။ သင်္ချာပညာရပ်နဲ့ ကွန်ပျူတာတွေ ရဲ့ လုပ်ဆောင်နိုင်စွမ်းတွေကို ပေါင်းစပ်လိုက်တဲ့အခါ အလွန်အလွန်ခန့်မှန်းရခက်တဲ့ ဝှက်စာတွေကို ရေးသားနိုင်နေပါပြီ။ ဘက်ညီဝှက်စာဗေဒရဲ့ သမိုင်းကြောင်းက အလွန်ရှည်လျားပြီး လက်တွေ့အသုံးချ နိုင်တဲ့နည်းလမ်းတွေလည်း အများကြီးရှိပါတယ်။

ဒါပေမဲ့လည်း ဘက်ညီဝှက်စာဗေဒမှာ အားနည်းချက်အချို့ရှိနေပါတယ်။ တကယ်လို့ တစ်စုံတစ်ယောက်က ဂျူလီယာနဲ့ဆီဇာတို့ ဝှက်စာဖြည်တဲ့သော့ကို မျှသုံးတဲ့အချိန်ကို စောင့်လို့ သော့ကိုခိုးပြီး ဝှက်စာဖြည်မယ်ဆိုရင် ဘယ်လိုလုပ်မလဲ။ ဂျူလီယာနဲ့ ဆီဇာတို့အကြား ဝှက်စာကုဒ်ကိုပြောချိန်ကို စောင့်ပြီး ခိုးနားထောင်ရင်ရော ဘယ်လိုလုပ်မလဲ။ ဒါမှမဟုတ် ဂျူလီယာနဲ့ ဆီဇာတို့က ကမ္ဘာကြီးရဲ့ တစ်ဘက်စီရောက်နေပြီး လူချင်းတွေ့ဖို့ အစီအစဉ်မရှိရင်ရော ဘယ်လိုလုပ်မလဲ။

ဒီပြဿနာတွေကို သူတို့နှစ်ယောက်ဘယ်လို ကျော်လွှားလို့ရမလဲ။

ဂျူလီယာနဲ့ဆီဇာကအများသုံးစကားဝှက်သော့ပါဝှက်စာဗေဒ public key cryptography ကို သုံးမယ်ဆိုပါစို့။ ဂျူလီယာနဲ့ ဆီဇာဆီကနေ ကုဒ်ဖြည်တဲ့သော့ကို ကြားလူတစ်ယောက်က ခိုးယူဖို့ မဖြစ်နိုင်တော့ပါဘူး။ ဘာလို့လဲဆိုတော့ ကုဒ်ဖြည်တဲ့သော့က တစ်ချောင်းတည်းမဟုတ်လို့ နှစ်ယောက်အကြား မျှသုံးစရာမလိုတော့လိုပါ့။ အများသုံးစကားဝှက်သော့ပါဝှက်စာဗေဒမှာ ကုဒ်ဖြင့်ပြောင်းလဲခြင်း အတွက်ကသော့တစ်ချောင်း၊ ကုဒ်ကိုပြန်ဖြည်ဖို့အတွက်က သပ်သပ်သော့တစ်ချောင်းသုံးပါတယ်။

အများသုံးစကားဝှက်သော့ပါကုဒ်ဖြင့် ပြောင်းလဲခြင်း- သော့နှစ်ချောင်းပုံပြင်

ပြဿနာကို အသေးစိတ်လေ့လာကြည့်ရအောင်။ ဘက်ညီဝှက်စာဖြည်သော့ကို တခြားသူတစ်ယောက်က

စောင့်ကြည့်ခိုးယူတာမျိုးမလုပ်နိုင်အောင် ပေးပို့သူကဘယ်လိုလုပ်နိုင်မလဲ။ ပေးပို့သူနဲ့ လက်ခံသူက တစ်ယောက်တစ်နေရာစီ ဖြစ်နေပြီး သူတို့ကိုစောင့်ကြည့်တဲ့သူမရှိဘဲ သူတို့နှစ်ယောက်ဘယ်လိုစကားပြောမလဲ။

အများသုံးစကားဝှက်သော့ပါဝှက်စာဗေဒ cryptography (ဘက်မညီဝှက်စာဗေဒ) ကတော့ ဒီပြဿနာတွေအတွက် တိကျသေချာတဲ့အဖြေထုတ်ထားပါတယ်။ ဆက်သွယ်သူနှစ်ယောက်မှာ တစ်ယောက်စီအတွက် သော့နှစ်ချောင်းစီဖန်တီးထားပါတယ် - အများသုံးစကားဝှက်သော့နှင့် ကိုယ်ပိုင်စကားဝှက်သော့ပါ။ ဒီသော့နှစ်ချောင်းကို ချိတ်ဆက်ထားပြီး သော့နှစ်ချောင်းမှာ သင်္ချာဂုဏ်သတ္တိရှိတဲ့ ကိန်းဂဏန်း အကြီးကြီးတွေပါပါတယ်။ သင်က အများသုံးစကားဝှက်သော့ကို အသုံးပြုပြီး မက်ဆေ့ချ်ကို ဝှက်စာပြောင်းပို့ရင် လက်ခံသူက သူ့မှာရှိတဲ့ ကိုယ်ပိုင်စကားဝှက်သော့နဲ့ပြန်ဖြည်လို့ရပါတယ်။

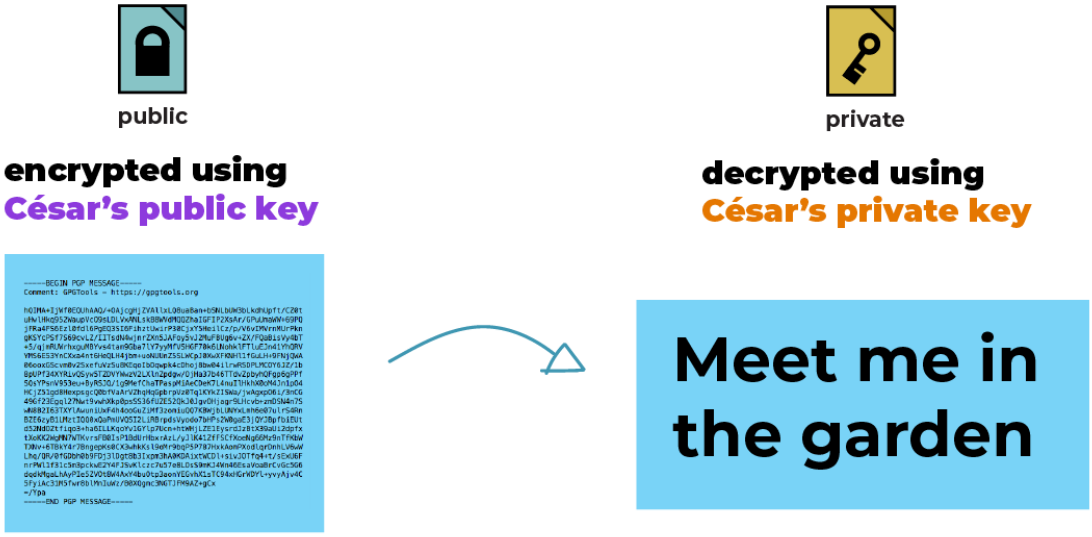
အခုတော့ ဂျူလီယာနဲ့ဆီဇာတို့က စာပို့မယ့်အစား သူတို့ကွန်ပျူတာတွေမှာ အများသုံးစကားဝှက်သော့ပါ ဝှက်စာဗေဒ public key cryptography ကိုသုံးပြီး ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ်တွေပို့ နေပါပြီ။ အတန်းဖော်တွေကိုသုံးပြီး စာတိုပို့မယ့်အစား ကွန်ပျူတာတွေသုံးပြီး မက်ဆေ့ချ်ပို့နေပါပြီ။ ဂျူလီယာနဲ့ဆီဇာအကြားကြားခံဖြစ်လာသူတွေက ဝိုင်ဖိုင်ပို့ဂ်တွေ၊ အင်တာနက်ဝန်ဆောင်မှုပေးသူတွေနဲ့ သူတို့ရဲ့ အီးမေးလ်ဆာဗာတွေပါ။ လက်တွေ့မှာ ဂျူလီယာနဲ့ဆီဇာတို့အကြားဆက်သွယ်မှုလုပ်နိုင်ဖို့ ကြားခံချိတ်ဆက်ပေးတဲ့ကွန်ပျူတာအရေအတွက်က ရာပေါင်းများစွာဖြစ်နိုင်ပါတယ်။ ဒီကြားခံတွေက မက်ဆေ့ချ်ကိုတစ်ခါလက်ဆင့်ကမ်းတိုင်း တစ်ခါမိတ္တူပွားပြီး ပေးပို့ပါတယ်။

သူတို့နှစ်ယောက်အနေနဲ့ နှစ်ယောက်ကြား ဆက်သွယ်နေတယ်ဆိုတာကို ကြားခံတွေသိတာခံနိုင်ပေမဲ့ သူတို့ပြောနေတဲ့ အကြောင်းအရာတွေကိုတော့ ဘယ်သူမှမသိစေချင်ပါဘူး။

ပထမဆုံးအနေနဲ့ ဂျူလီယာက ဆီဇာရဲ့ အများသုံးစကားဝှက်သော့ကိုရယူဖို့လိုပါတယ်။ ဆီဇာက သူ့ရဲ့ အများသုံးစကားဝှက်သော့ကို မလုံခြုံနဲ့ နည်းလမ်း(ဥပမာ- ကုဒ်နဲ့ပြောင်းလဲထားခြင်းမရှိတဲ့မေးလ်) နဲ့ ပို့လိုက်တယ်။ သူ့သော့ ကိုကြားခံတွေသိသွားမှာမစိုးရိမ်ဘူး။ ဘာလို့လဲဆိုတော့ အဲဒီသော့က အများသုံးစကားဝှက်သော့ဖြစ်နေလို့ပါ။ ဒီနေရာမှာ သော့ဆိုတာ တကယ့်သော့မဟုတ်ဘဲ ကုဒ်နံပါတ်တွေဆိုတာကို သတိပြုပါ။ ဆီဇာက သူ့ရဲ့ အများသုံးစကားဝှက်သော့ကို နည်းလမ်းအမျိုးမျိုးနဲ့ပို့လိုက်တာမို့ ကြားခံတွေက သူတို့ရဲ့ကိုယ်ပိုင် အများသုံးစကားဝှက်သော့တွေကို ဂျူလီယာ့ဆီကို ကြားဖြတ်ပို့လို့မရတော့ပါဘူး။

ဂျူလီယာက ဆီဇာ့ရဲ့ အများသုံးစကားဝှက်သော့ပါတဲ့ဖိုင်ကို လက်ခံရရှိတဲ့အခါ ဆီဇာ့ဆီကို ကုဒ်နဲ့ပြောင်းလဲထား တဲ့ မက်ဆေ့ချ်ကိုပို့လို့ရပြီလေ။ ဂျူလီယာက “ပန်းခြံမှာဆုံရအောင်” လို့ရေးပို့လိုက်ပါတယ်။

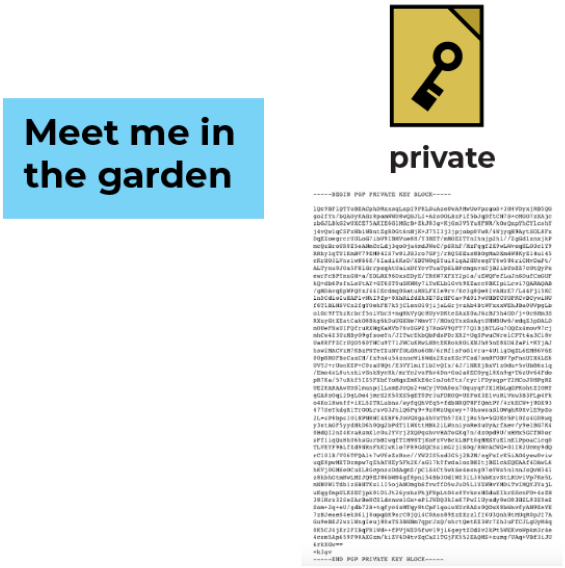
ဂျူလီယာက ကုဒ်နဲ့ပြောင်းလဲထားတဲ့မက်ဆေ့ချ်ကို ပို့လိုက်ပါတယ်။ အဲဒီမက်ဆေ့ချ်က ဆီဇာ့ တစ်ယောက်တည်းအတွက် ကုဒ်နဲ့ပြောင်းလဲထားတာပါ။



ဂျူလီယာနဲ့ဆီဇာနှစ်ယောက်ပဲ မက်ဆေ့ချ်ကိုဖတ်လို့ရပြီး ကျန်တဲ့သူတွေအတွက်တော့ ဖတ်မရတဲ့စာကြောင်းဖြစ်နေပါတယ်။ ကြားခံတွေကာတေ့ အချက်အလက်တွေအကြောင်းရှင်းပြတဲ့အချက်အလက် metadata တွေဖြစ်တဲ့ ပေးပို့တဲ့အကြောင်းအရာခေါင်းစဉ်၊ နေ့စွဲ၊ ပေးပို့သူနဲ့ လက်ခံသူစတာတွေကို မြင်ရမှာပါ။

ဂျူလီယာ (ပေးပို့သူ) နဲ့ ဆီဇာဖတ်လို့ရဖို့ရည်ရွယ်ပြီး ဆီဇာ့အများသုံးစကားဝှက်သော့နဲ့ မက်ဆေ့ချ်ကို ကုဒ်ဖြင့်ပြောင်းလဲထားတာဖြစ်လို့ သူတို့နှစ်ယောက်ပဲ မက်ဆေ့ချ်ကို ဖတ်လို့ရပါတယ်။

ဆီဇာက သူ့ရဲ့ ကိုယ်ပိုင်စကားဝှက်သော့ကိုသုံးပြီး မက်ဆေ့ချ်ကိုဖတ်လို့ရပါတယ်။



ပြန်ချုပ်ရရင် -

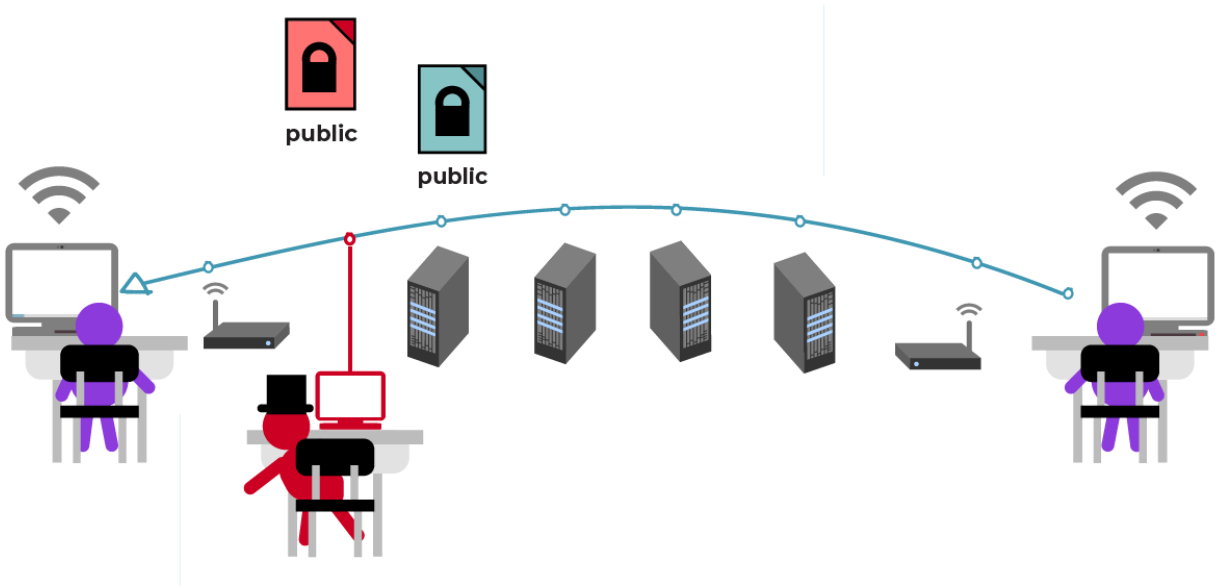
- အများသုံးစကားဝှက်သော့ပါ ဝှက်စာဗေဒနည်းလမ်းက အများသုံးစကားဝှက်သော့ကို လုံခြုံမှုမရှိတဲ့ လမ်းကြောင်းတွေကနေတဆင့် ပေးပို့လို့ရအောင် လုပ်ထားတယ်။
- လက်ခံမယ့်သူရဲ့ အများသုံးစကားဝှက်သော့က သင့်လက်ထဲမှာရှိရင် သူတို့ဆီကို ကုဒ်ဖြင့်ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ် တွေပို့လို့ရတယ်။
- သင့်ရဲ့ကိုယ်ပိုင်စကားဝှက်သော့ကိုတော့ သင့်ဆီပို့လာတဲ့ ကုဒ်ဖြင့်ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ်တွေကို ပြန်ဖြည်ဖို့အတွက် သုံးပါတယ်။
- ကြားခံများ - ဥပမာ အီးမေလ်ဝန်ဆောင်မှုပေးသူများ၊ အင်တာနက်ဝန်ဆောင်မှုပေးသူများနဲ့ နက်ဝေါ့ခ်မှာရှိနေသူများအနေနဲ့ အချက်အလက်တွေအကြောင်းရှင်းပြတဲ့ အချက်အလက်တွေ ဖြစ်တဲ့ ဘယ်သူကဘယ်သူ့ဆီဘာကိုပို့တယ်၊ ဘယ်အချိန်မှာလက်ခံရရှိတယ်၊ ပေးပို့တဲ့ အကြောင်းအရာခေါင်းစဉ်ကဘာလဲနဲ့ အဲဒီမက်ဆေ့ချ်ကို ကုဒ်နဲ့ပြောင်းလဲထားတယ်စသည်ဖြင့် မြင်တွေ့နိုင်ပါတယ်။

နောက်ထပ်ပြဿနာတစ်ခု - အယောင်ဆောင်ခြင်းဆိုတာဘာလဲ။

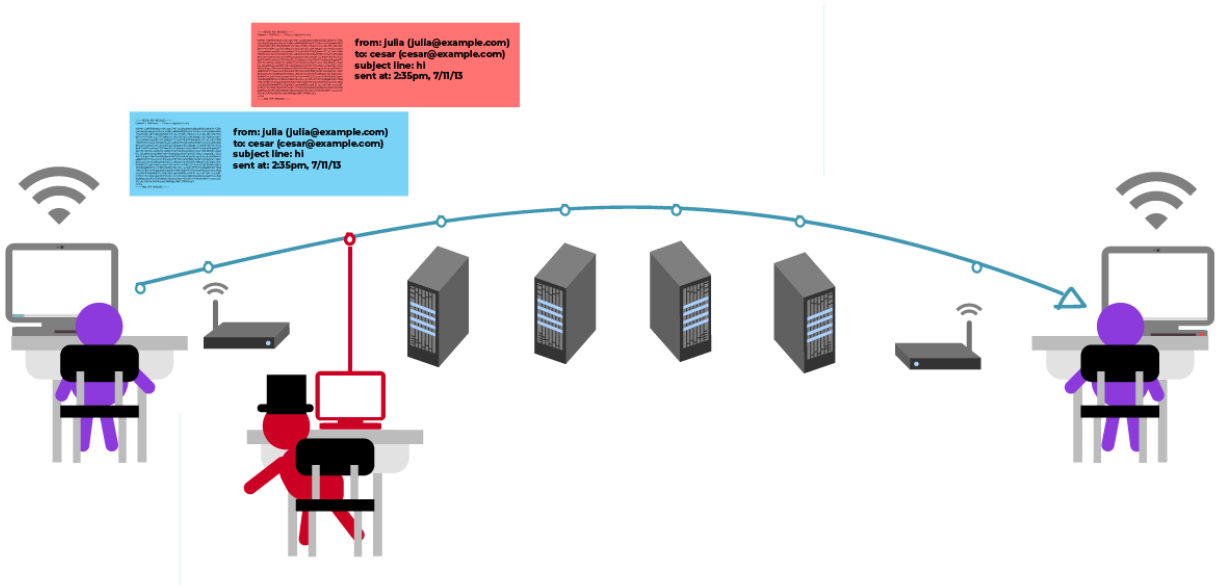
ဂျူလီယာနဲ့ဆီဇာတို့ရဲ့ဥပမာမှာဆိုရင် ကြားခံတွေက သင့်ရဲ့ အချက်အလက်အကြောင်းရှင်းပြတဲ့ အချက်အလက်တွေ metadata ကိုအချိန်မရွေး မြင်တွေ့ရပါမယ်။

ဒီကြားခံတွေထဲကတစ်ခုက မကောင်းတဲ့သူဆိုရင် ဘာဖြစ်နိုင်မလဲ။ မကောင်းတဲ့သူ ဆိုတာကို အဓိပ္ပါယ်ဖွင့်ရရင် သင့်ရဲ့ အချက်အလက်တွေကို ခိုးယူဖို့ကြိုးစားတာပဲဖြစ်ဖြစ်၊ တနည်းနည်းနဲ့ အနှောင့်အယှက်ပြုပြီး သင့်ကို ထိခိုက်အောင်လုပ်ချင်တဲ့သူကို ဆိုလိုတာဖြစ်တယ်။ အဲဒီလိုလူတစ်ယောက်က ဂျူလီယာနဲ့ ဆီဇာအကြားက မက်ဆေ့ချ်တွေကို စောင့်ကြည့်ထောက်လှမ်းနေတယ်ဆိုပါစို့။

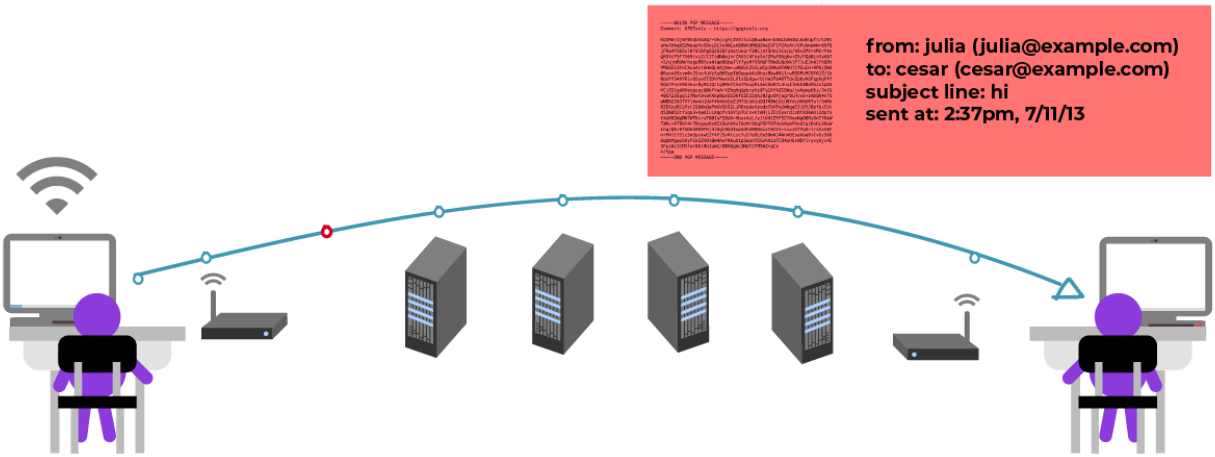
အဲဒီမကောင်းတဲ့သူက ဂျူလီယာ့ကို လှည့်ဖျားပြီး အများသုံးစကားဝှက်သော့အမှားကြီးကို သူမဆီရောက်အောင် လုပ်လိုက်တယ်ဆိုပါစို့။ ဂျူလီယာကတော့ ဆီဇာ့ရဲ့ အများသုံးစကားဝှက်သော့လို့ ထင်ပြီး မက်ဆေ့ချ်ပို့လိုက်ရင် ဂျူလီယာ့မက်ဆေ့ချ်က အဲဒီမကောင်းတဲ့သူဆီအရင်ရောက်သွားပြီး အဲဒီကမှတဆင့် ဆီဇာ့ဆီထပ်ပို့ ပေးလိုက်မှာဖြစ်တယ်။



မကောင်းတဲ့ကြားခံလူက ဆီဇာ့ဆီမပို့ခင် မက်ဆေ့ချ်မှာပါနေတဲ့ အကြောင်းအရာတွေကိုပါ ပြောင်းလဲနိုင်ပါသေးတယ်။



များသောအားဖြင့် မက်ဆေ့ချ်ကို ပြောင်းလဲခြင်းမရှိဘဲ ပေးပို့တတ်ပါတယ်။ မကောင်းတဲ့ကြားခံလူက မက်ဆေ့ချ်ကို မပြင်ဘဲ မူလအတိုင်းဆီဇာ့ဆီပို့ပေးလိုက်ပါတယ်။ ဆီဇာက မက်ဆေ့ချ်အတိုင်း ဂျူလီယာနဲ့တွေ့ဖို့ ပန်းခြံကိုသွားပါမယ်။ သူတို့နှစ်ယောက်မမျှော်လင့်တာက မကောင်းတဲ့ကြားခံလူကလည်း အဲဒီပန်းခြံကို ရောက်နှင့်နေတာပါပဲ။



ဒီလိုတိုက်ခိုက်မှုမျိုးကို ကြားခံလူမှတိုက်ခိုက်ခြင်း man-in-the-middle attack လို့ခေါ်ပါတယ်။ နောက်တစ်မျိုးအနေနဲ့ ကြားခံစက်မှ တိုက်ခိုက်ခြင်း machine-in-the-middle attack လို့လည်း ခေါ်ပါတယ်။

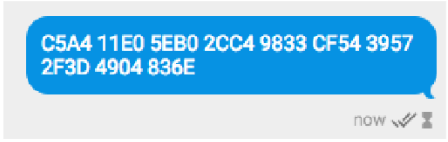
ကံကောင်းတာတစ်ခုက အများသုံးစကားဝှက်သော့ပါ ဝှက်စာဗေဒစနစ်မှာ ကြားခံလူမှ တိုက်ခိုက်ခြင်းကို ကာကွယ်ဖို့နည်းလမ်းရှိနေတာပါ။

အများသုံးစကားဝှက်သော့ပါဝှက်စာဗေဒစနစ်မှာ လူတစ်ယောက်ရဲ့ ဒီဂျစ်တယ်ကိုယ်ရေးအချက်အလက်ကို ပြင်ပကိုယ်ရေးအချက်အလက်နဲ့ တူ/မတူ တိုက်ဆိုင်စစ်ဆေးတဲ့စနစ်ဖြစ်တဲ့ လက်ဗွေနဲ့ အတည်ပြုသက်သေခံခြင်း “fingerprint verification” ပါဝင်ပါတယ်။ ဖြစ်နိုင်ရင်တော့ သင့်မိတ်ဆွေနဲ့ သင်တို့နှစ်ယောက်အပြင်မှာတွေ့နိုင်ရင်ကောင်းတာပေါ့။ သင့်ရဲ့ အများသုံးစကားဝှက်သော့ရဲ့ လက်ဗွေဖြစ်တဲ့ ကိန်းဂဏန်းအက္ခရာစဉ်မှာပါဝင်တဲ့ နံပါတ်အားလုံးကို သင့်မိတ်ဆွေဆီမှာရှိတဲ့ သင့်ရဲ့ အများသုံးစကားဝှက်သော့မှာပါတဲ့ နံပါတ်တွေနဲ့ တစ်လုံးချင်း တိုက်ဆိုင်စစ်ဆေးဖို့လိုပါတယ်။ နည်းနည်းတော့ အချိန်ကြာပေမဲ့ လုပ်သင့်တဲ့ကိစ္စဖြစ်ပါတယ်။

အစ - အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းစနစ်ကို အသုံးပြုတဲ့ အက်ပ်တွေမှာ လက်ဗွေကို စစ်တဲ့ နည်းလမ်းတစ်မျိုးမျိုးတော့ ပါတတ်ပါတယ်။ အချို့အက်ပ်တွေမှာဆိုရင် သင့်စခရင်ပေါ်ရှိတဲ့ လက်ဗွေမှာပါတဲ့ အက္ခရာတွေကို တစ်လုံးချင်းသေချာဖတ်ပြီး သင့်မိတ်ဆွေစခရင်ပေါ်က လက်ဗွေနဲ့တိုက်ဆိုင်စစ်ဆေးနိုင်ပါတယ်။ အချို့အက်ပ်တွေကျတော့ သင့်မိတ်ဆွေစခရင်မှာပေါ်လာတဲ့ QR codeကို သင့်စက် ပစ္စည်းနဲ့ ဖတ်ပြီး သူတို့ရဲ့စက်ကို အတည်ပြုပေးတာပါ။ ဒီဥပမာမှာတော့ ဂျူလီယာနဲ့ ဆီဇာတို့နှစ်ယောက် အပြင်မှာတွေ့ပြီး ဖုန်းတွေက လက်ဗွေကို အပြန်အလှန်စကင်ဖတ်ပြီး အတည်ပြုစစ်ဆေး နေတာပါ။

သင့်အနေနဲ့ လူချင်းမတွေ့နိုင်ဘူးဆိုရင်တော့ လက်ဗွေကို အခြားလုံခြုံတဲ့လမ်းကြောင်း၊ ဥပမာ အစ-အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို အသုံးပြုပြီး မက်ဆေ့ချ်ပို့နိုင်တဲ့ အက်ပ် (သို့မဟုတ်) ချက်တင် စနစ် (သို့မဟုတ်) HTTPS ဆိုက်ကို အသုံးပြုပြီးပို့လို့ရပါတယ်။

အောက်မှာဖော်ပြထားတဲ့ ပုံမှာဆိုရင် ဆီဇာကသူ့ရဲ့ အများသုံးလက်ဗွေသော့ကို သူ့စမတ်ဖုန်းမှာ အစ-အဆုံးကုဒ်ဖြင့် ပြောင်းလဲနိုင်တဲ့ အက်ပ်ကို အသုံးပြုပြီး ဂျူလီယာဆီပို့နေတာပါ။



အနှစ်ချုပ်ပြန်ပြောရရင်

- ကြားခံလူမှုတိုက်ခိုက်ခြင်းဆိုတာက သင်ကလူတစ်ယောက်ဆီပို့လိုက်တဲ့ မက်ဆေ့ချ်ကို အခြားသူတစ်ဦးက ကြားဖြတ်ခိုးယူတာကိုခေါ်ပါတယ်။ တိုက်ခိုက်သူက သင့်မက်ဆေ့ချ်ကို ပြောင်းလဲပြီး လက်ခံသူထံဆက်ပို့တာဖြစ်နိုင်သလို ကြားဖြတ်ခိုးကြည့်ပြီး မက်ဆေ့ချ်ကို မူလအတိုင်း လက်ခံသူဆီ ဆက်ပို့တာလည်းဖြစ်နိုင်ပါတယ်။
- အများသုံးစကားဝှက်သော့ပါ ဝှက်စာဗေဒမှာ ပေးပို့သူရဲ့ ကိုယ်ရေးအချက်အလက်ကို အတည်ပြုနိုင်တဲ့ နည်းလမ်းတွေပါဝင်လို့ ကြားခံလူမှုတိုက်ခိုက်မှုများကို အကာအကွယ်ပေးနိုင်ပါတယ်။ လက်ဗွေအတည်ပြုစစ်ဆေးခြင်းနည်းလမ်းနဲ့ တိုက်ဆိုင်စစ်ဆေး အတည်ပြုနိုင်ပါတယ်။
- သင့်မိတ်ဆွေဆီပို့တဲ့ မက်ဆေ့ချ်ကို ကုဒ်ဖြင့်ပြောင်းလဲခြင်း encrypt အပြင် သင့်မိတ်ဆွေရဲ့ သော့မှာ အများသုံးလက်ဗွေသော့ပါဝင်တာကြောင့် အဲဒီလက်ဗွေကိုသုံးပြီး မက်ဆေ့ချ်ပို့ သူက သင့်မိတ်ဆွေဟုတ်/မဟုတ်ကို အတည်ပြုစစ်ဆေးနိုင်ပါတယ်။
- ကိုယ်ပိုင်စကားဝှက်သော့ကို ကုဒ်ဖြင့်ပြောင်းလဲထားသော မက်ဆေ့ချ်တွေအတွက်သာမက မက်ဆေ့ချ်တွေမှာပါရှိတဲ့ သင့်ဒစ်ဂျစ်တယ် လက်မှတ်အဖြစ်လည်း သုံးနိုင်ပါတယ်။

တုမရတဲ့ လက်မှတ်

အများသုံးစကားဝှက်သော့ပါဝှက်စာဗေဒကိုသုံးမယ်ဆိုရင် သင့်အနေနဲ့ ဝှက်စာဖြည်တဲ့သော့ကို
လက်ခံသူဆီ ခိုးကြောင်ခိုးဝှက်ပို့စရာမလိုပါဘူး။ ဘာလို့လဲဆိုတော့ အဲဒီလူရဲ့
ကိုယ်ပိုင်စကားဝှက်သော့က ဝှက်စာဖြည်တဲ့သော့ဖြစ်ပြီး သူ့လက်ထဲမှာအစကတည်းကရှိနေတာမို့ပါ။
မက်ဆေ့ချ်တွေကို ကုဒ်နဲ့ပြောင်းလဲပေးဖို့ လက်ခံသူဆီက အများသုံး သော့ပဲ
သင့်လက်ထဲမှာရှိဖို့လိုတာပါ။ အဲဒါကလည်း လွယ်ပါတယ်။ အများသုံး သော့ဖြစ်ကို
ကုဒ်နဲ့ပြောင်းလဲဖို့ပဲသုံးနိုင်ပြီး ပြန်ဖြည်ဖို့မသုံးနိုင်လို့ ဘယ်သူ့ကိုမဆို အလွယ်တကူပို့လို့ ရပါတယ်။

ဒီထက်ကောင်းတာရှိပါသေးတယ်။ အများသုံးစကားဝှက်သော့ကိုသုံးပြီး မက်ဆေ့ချ်ကို
ကုဒ်နဲ့ပြောင်းလဲထားရင် သူရဲ့ အတွဲအစပ်ဖြစ်တဲ့ ကိုယ်ပိုင်စကားဝှက်သော့နဲ့ပဲ
ကုဒ်ကိုပြန်ဖြည်လို့ရတယ်ဆိုတာသင်သိပြီးဖြစ်ပါတယ်။ အဲ့ဒါ ရဲ့ အပြန်အလှန်ကလည်း
အလုပ်ဖြစ်ပါတယ်။ သင့်အနေနဲ့ မက်ဆေ့ချ်တစ်ခုကို ကိုယ်ပိုင်စကားဝှက်သော့သုံးပြီး
ကုဒ်နဲ့ပြောင်းလဲထားရင်လည်း သူရဲ့အတွဲအစပ်ဖြစ်တဲ့ အများသုံးစကားဝှက်သော့နဲ့ပဲ
ပြန်ဖြည်လို့ရတယ်ဆိုတာပါ ပဲ။

ဒီအချက်က ဘယ်လိုအသုံးဝင်လည်းဆိုတာဆက်ကြည့်ရအောင်။ သာမန်ကြည့်ရင်တော့
သင့်ရဲ့ကိုယ်ပိုင်စကားဝှက်သော့ကိုသုံးပြီး ကုဒ်နဲ့ပြောင်းလဲထားတဲ့မက်ဆေ့ချ်ကို
သင့်အများသုံးစကားဝှက်သော့ကို ရရှိထားသူတိုင်းက ပြန်ဖြည်လို့ ရတာမို့ သိပ်အသုံးမဝင်သလိုပါပဲ။
သင်က “အဇူးလ်ကို ဒေါ်လာ ၁၀၀ပေးဖို့ ကတိပေးတယ်” ဆိုတဲ့
ကိုယ်ပိုင်စကားဝှက်သော့ကိုသုံးပြီးရေးထားတဲ့ မက်ဆေ့ချ် ဖြစ်ကို ရေးလိုက်တယ်ဆိုပါစို့။ သင့်ရဲ့
အများသုံး စကားဝှက်သော့ရှိသူတိုင်းက အဲဒီ မက်ဆေ့ချ်ကို ပြန်ဖြည်လို့ရပေမဲ့ သင်ကလွဲလို့
အခြားသူတစ်ယောက်က အဲဒီ မက်ဆေ့ချ်ကိုရေးလို့မရဘူး။ ဆိုလိုတာက သင့်အနေနဲ့
သင့်ကိုယ်ပိုင်စကားဝှက်သော့ကို လုံခြုံစွာသိမ်းထားတယ် ဆိုရင် အခြားတစ်ယောက်က
အဲဒီမက်ဆေ့ချ်ကိုရေးလို့မရတဲ့အတွက် အဲဒီမက်ဆေ့ချ်ကို ဖတ်လို့ရသူ တိုင်းက
သင်ရေးထားတာဖြစ်ကြောင်း အတည်ပြုလို့ရတယ်။ အဲဒါက အပြင်လောကမှာ လက်မှတ်ထိုး သလိုပဲ
သင့်မက်ဆေ့ချ်တိုင်းအတွက် ဒစ်ဂျစ်တယ်လက်မှတ်လို အလုပ်လုပ်ပါတယ်။

ဒီနည်းလမ်းက ကြားဖြတ်ပြီးသင့်မက်ဆေ့ချ်ကို ပြောင်းချင်သူတွေကို ကာကွယ်ပြီးဖြစ်သွားပါတယ်။
အခြားတစ်ယောက်က သင့်မက်ဆေ့ချ်ဖြစ်တဲ့ “အဇူးလ်ကို ဒေါ်လာ ၁၀၀ ပေးဖို့ ကတိပေးတယ်” အစား
“မင်းဂ်ကို ဒေါ်လာ ၁၀၀ ပေးဖို့ ကတိပေးတယ်” လို့ ကြားဖြတ်ပြောင်းချင်ရင်တောင်
သင့်ကိုယ်ပိုင်စကားဝှက်သော့ မရှိလို့ ပြောင်းလို့ရမှာမဟုတ်ပါဘူး။ ဒါ့ကြောင့် သေချာတာတစ်ခုက
မက်ဆေ့ချ်တစ်ခုမှာ ဒီဂျစ်တယ် လက်မှတ်ပါနေပြီဆိုရင် လမ်းမှာ တစုံတယောက်ကကြားဖြတ်ပြီး
ပြောင်းလဲထားတာမျိုး မရှိဘူးဆို တာပါပဲ။

အတိုချုပ်- အများသုံးစကားဝှက်သော့နှစ်ချောင်းပါဝှက်စာဗေဒကို အသုံးပြုခြင်း

ရှေ့မှာပြောခဲ့တာတွေကို ပြန်ချုပ်ရရင် အများသုံးစကားဝှက်သော့ပါဝှက်စာဗေဒမှာ သင့်လက်ထဲမှာ ရှိတဲ့ အများသုံးစကားဝှက်သော့တွေရဲ့ပိုင်ရှင်တိုင်းဆီကို ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ်တွေပို့လို့ရပါတယ်။

သင့်ရဲ့ကိုယ်ပိုင်အများသုံးစကားဝှက်သော့ကို သိရှိသူတိုင်းက

- သင့်ဆီကို ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ်တွေပို့လို့ရပြီး သင့်အနေနဲ့ ကိုယ်ပိုင်ကိုယ်ပိုင်စကားဝှက်သော့ ကိုသုံးပြီး ပြန်ဖြည်လို့ရပါတယ်။
- သင့်မက်ဆေ့ချ်တွေကို သင့်ရဲ့ကိုယ်ပိုင်ကိုယ်ပိုင်စကားဝှက်သော့နဲ့ လက်မှတ်ထိုးလို့ရပြီး လက်ခံရသူတိုင်း အနေနဲ့ သင့်ဆီကပို့တယ်ဆိုတာကို အတည်ပြုလို့ရစေပါတယ်။

ဒါ့အပြင် သင့်အနေနဲ့ တစုံတယောက်ရဲ့ အများသုံးစကားဝှက်သော့ကိုသိတယ်ဆိုရင် -

- သူတို့လက်မှတ်ပါတဲ့ မက်ဆေ့ချ်ကို ပြန်ဖြည်လို့ရပြီး သူတို့ဆီကပို့တယ်ဆိုတာကို အတည်ပြုလို့ရပါတယ်။

အခုလောက်ဆိုရင်တော့ အများသုံးစကားဝှက်သော့ပါ ဝှက်စာဗေဒမှာ သင့်ရဲ့အများသုံးစကားဝှက်သော့ကို လူအများသိလေလေ အလုပ်ဖြစ်လေလေဆိုတာ ရှင်းလောက်ပါပြီ။ အများသုံးစကားဝှက်သော့ကို သင့်လိပ်စာ၊ ဖုန်းနံပါတ်ပေးသလို လူများများဆီပေးထားလေလေ၊ သင့်ဆီကို မက်ဆေ့ချ်ပို့တဲ့အခါ ကုဒ်နဲ့ပြောင်းလဲ ထားတဲ့ မက်ဆေ့ချ်တွေပို့ဖို့ ဖြစ်နိုင်ခြေများလေလေပါပဲ။ သင်နဲ့ဆက်သွယ်လိုသူတိုင်းကို သင့်ရဲ့ အများသုံးစကားဝှက်သော့ကို ပေးထားနိုင်ပါတယ်။ အများသုံးဖြစ်တာမို့ ဘယ်သူသိသိ ကိစ္စမရှိပါဘူး။

အဲဒီအများသုံးစကားဝှက်သော့တိုင်းမှာ သူနဲ့တွဲထားတဲ့ ကိုယ်ပိုင်စကားဝှက်သော့ရှိပါတယ်။ ကိုယ်ပိုင်စကားဝှက်သော့ကိုတော့ ဘယ်သူမှ မသိအောင် သိမ်းထားရမယ့်သော့၊ ကိုယ့်တစ်ယောက်တည်းဆီမှာပဲထားရမယ့်သော့လို့မှတ်ထားဖို့လိုပါတယ်။ အဲဒီသော့နဲ့ မက်ဆေ့ချ်တွေကို ကုဒ်နဲ့ပြောင်းလဲတာရော၊ ပြန်ဖြည်တာရောလုပ်လို့ရပါတယ်။

သင့်ရဲ့ ကိုယ်ပိုင်စကားဝှက်သော့ကိုတော့ လုံခြုံတဲ့နေရာမှာ သိမ်းဆည်းထားဖို့လိုပါတယ်။ သင့်စက်ပစ္စည်းထဲမှာ သိမ်းထားတဲ့သင့်ရဲ့ ကိုယ်ပိုင်စကားဝှက်သော့ကို မတော်တဆများဖျက်လိုက်မိရင် သင့်အနေနဲ့ မက်ဆေ့ချ်တွေကို ကုဒ်နဲ့ပြောင်းတာရော၊ ပြန်ဖြည်တာရောလုပ်နိုင်တော့မှာမဟုတ်ပါဘူး။ သင့်သော့ကို အခြားသူတစ်ယောက်က မိတ္တူပွားယူလိုက်ရင် (သင့်ကွန်ပျူတာထဲကခိုးယူရင်/ malware နဲ့ခိုးယူရင်/ မတော်တဆသူများဆီပို့မိရင်) အခြားသူတွေက သင့်ရဲ့ကုဒ်နဲ့ပြောင်းလဲထားတဲ့

မက်ဆေ့ချ်တွေကို ဖတ်လို့ရ သွားပါလိမ့်မယ်။ ဒါ့အပြင် သင့်ရဲ့ဒီဂျစ်တယ်လက်မှတ်ထိုးပြီး မက်ဆေ့ချ်တွေကို သင်ပို့သယောင် ဖန်တီးလို့ရသွားပါလိမ့်မယ်။

အစိုးရတွေအနေနဲ့ သူတို့ပစ်မှတ်ထားတဲ့လူတွေရဲ့ ကွန်ပျူတာတွေကို သိမ်းဆည်းပြီး ဒါမှမဟုတ် တိုက်ရိုက် (သို့မဟုတ်) ဖစ်ရှင်းကတဆင့် malware တိုက်ခိုက်မှုလုပ်ဆောင်ပြီးကိုယ်ပိုင်စကားဝှက်သော့တွေကို ခိုးယူတာမျိုး လုပ်တာမကြာခဏကြား ဖူးပါတယ်။ ဒီလိုလုပ်ဆောင်တာက ဝှက်စာဗေဒ cryptography မှာရှိတဲ့ ကိုယ်ပိုင်စကားဝှက်သော့ရဲ့ အကာအကွယ်ပေးနိုင်မှုကို လျော့ကျစေပါတယ်။ နှိုင်းပြောရရင် သင့်တံခါးမှာ ဖျက်လို့မရတဲ့ သော့ရှိပေမဲ့ တကယ်တမ်းကျ တစ်စုံတစ်ယောက်က သင့်သော့ကိုခါး ပိုက်နှိုက်၊ သော့တူပွား၊ သင့်အိပ်ကပ်ထဲ မသိအောင်ပြန်ထည့်ပြီး၊ သင်မသိဘဲသင့်အိမ်ထဲဝင်ထဲကို သော့ဖျက်စရာမလိုပဲ ဝင်လို့ရတယ်လို့ ပြောနေသလိုပါပဲ။

ဒီလိုအခြေအနေအတွက် အန္တရာယ်ဖြစ်နိုင်ခြေအဆင့်သတ်မှတ်မှု threat modeling ကို စနစ်တကျ လုပ်ဖို့လိုပါတယ်။ သင့်ရဲ့ကိုယ်ပိုင်စကားဝှက်သော့ကို တစ်စုံတစ်ယောက်က မရ ရတဲ့နည်းနဲ့ ယူမယ်လို့ သံသယ ရှိရင် အဲဒီသော့ကို ဘရောက်ဇာကနေတဆင့် အစ - အဆုံးကုဒ်နဲ့ ပြောင်းလဲခြင်းအတွက် end-to-end encryption မသုံးသင့်ဘူး။ ဆိုလိုတာက အဲဒီသော့ကို အခြားသူရဲ့ကွန်ပျူတာတွေဖြစ်တဲ့ (cloud တို့ ဆာဗာတို့) မှာ မသိမ်းမိစေဘဲ မိမိရဲ့ကိုယ်ပိုင်ကွန်ပျူတာ (သို့မဟုတ်) ဖုန်းထဲမှာပဲ သိမ်းထားသင့် ပါတယ်။

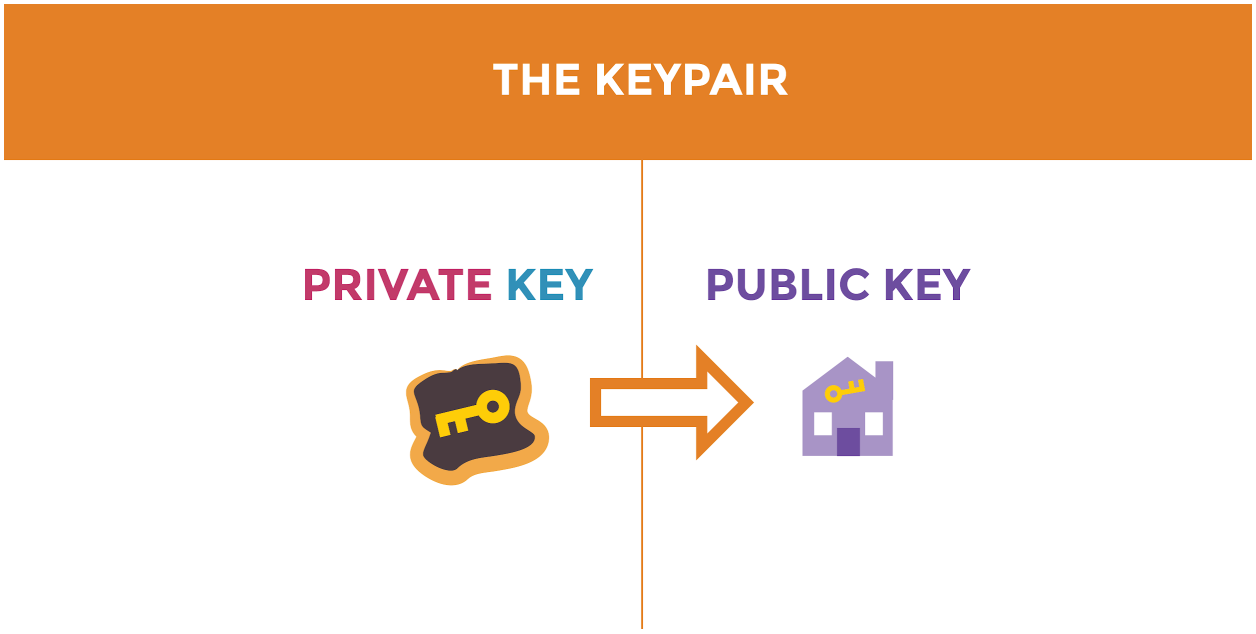
အများသုံးစကားဝှက်သော့ပါ ဝှက်စာဗေဒ ပြန်လှန်ဆန်းစစ်ခြင်းနှင့် တိကျသောဥပမာတစ်ခု - PGP

အခုအချိန်အထိ ဘက်ညီကုဒ်ဖြင့်ပြောင်းလဲခြင်း symmetric encryption နဲ့ အများသုံးစကားဝှက်သော့ဖြင့်ကုဒ်ပြောင်းလဲခြင်း public key encryption တွေကို သီးခြားဥပမာတွေအနေနဲ့ လေ့လာခဲ့ပြီးပါပြီ။ ဒီနေရာမှာနောက်တစ်ချက် သတိပြုမိစေလိုတာက အများသုံးစကားဝှက်သော့ဖြင့် ကုဒ်ပြောင်းလဲ ခြင်းမှာ ဘက်ညီကုဒ်ဖြင့်ပြောင်းလဲခြင်းကိုလည်း သုံးထားတယ်ဆိုတာပါပဲ။ အများသုံးစကားဝှက်သော့ဖြင့် ကုဒ်ပြောင်းလဲ ခြင်းမှာ တူညီတဲ့သော့ကိုသုံးပြီး ကုဒ်နဲ့ပြောင်းလဲတာရော၊ ပြန်ဖြည်တာရော လုပ်လို့ရပါတယ်။

PGP က ဘက်ညီဝှက်စာဗေဒကိုရော၊ အများသုံးစကားဝှက်သော့ပါဝှက်စာဗေဒ (ဘက်မညီ) နှစ်မျိုးလုံးကို အသုံးပြုတဲ့ လုပ်ထုံးလုပ်နည်း protocol ဥပမာတစ်ခုဖြစ်ပါတယ်။ PGP လို အစ - အဆုံးကုဒ်ဖြင့် ပြောင်းလဲခြင်းနည်းစနစ်တွေကို အသုံးပြုတာက အများသုံးစကားဝှက်သော့ပါ ဝှက်စာဗေဒ ရဲ့ လုပ်ဆောင်မှုတွေကို ပိုပြီးနားလည်လာစေပါလိမ့်မယ်။

သော့တွေဆိုတာ ဘာကိုဆိုလိုတာလဲ။ အဲဒီသော့တွေက တစ်ချောင်းနဲ့ တစ်ချောင်း ဘယ်လိုဆက်စပ်နေလဲ။

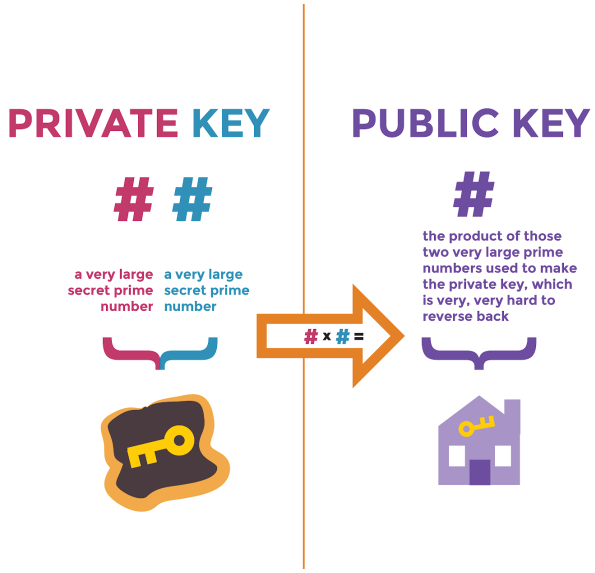
အများသုံးစကားဝှက်သော့ပါ ဝှက်စာဗေဒ Public key cryptography ကသော့နှစ်ချောင်းကို အခြေခံထားပါတယ်။ တစ်ချောင်းက ကုဒ်နဲ့ပြောင်းလဲတဲ့နေရာမှာသုံးပြီး နောက်တစ်ချောင်းကို ကုဒ်ပြန်ဖြည်ဖို့အတွက် သုံးပါတယ်။ အင်တာနက်ပေါ်မှာ မလုံခြုံတဲ့လမ်းကြောင်းကတဆင့် အခြားသူဆီပေးပို့လို့ရတဲ့သောကိုတော့ အများသုံးစကားဝှက်သော့လို့ခေါ်ပါတယ်။ အဲဒီသော့ကို ဘယ်သူ့ဆီမှာဖြစ်ဖြစ်၊ ဘယ်နေရာမှာဖြစ်ဖြစ်ပေးထားလို့ရပါတယ်။ သင့်ပို့တဲ့ ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ်တွေရဲ့ လုံခြုံမှုကို မထိခိုက်စေပါဘူး။

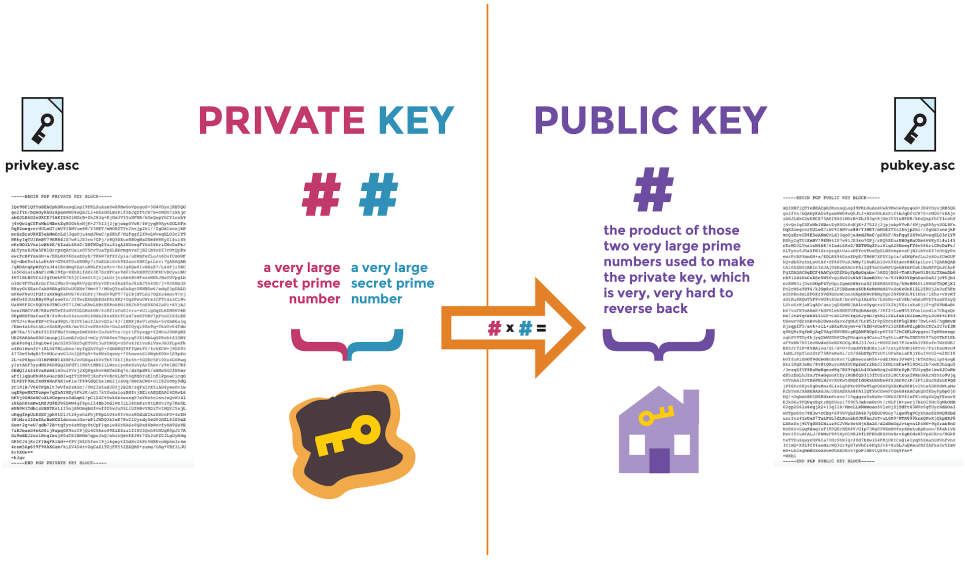


တခြားသူတွေဆီပေးထားရတဲ့သော့ကို အများသုံးစကားဝှက်သော့လို့ခေါ်ပါတယ်။ အများသုံးစကားဝှက်သော့ကို သင့်လိပ်စာ၊ ဖုန်းနံပါတ်ပေးသလို လူများများဆီပေးထားလေလေ၊ သင့်ဆီကို မက်ဆေ့ချ်ပို့တဲ့အခါ ကုဒ်နဲ့ပြောင်းလဲ ထားတဲ့encrypt မက်ဆေ့ချ်တွေပို့ဖို့ ဖြစ်နိုင်ခြေများလေလေပါပဲ။

အဲဒီအများသုံးစကားဝှက်သော့တိုင်းမှာ သူနဲ့တွဲထားတဲ့ ကိုယ်ပိုင်စကားဝှက်သော့ရှိပါတယ်။ ကိုယ်ပိုင်စကားဝှက်သော့ကိုတော့ ဘယ်သူမှ မသိအောင် သိမ်းထားရမယ့်သော့၊ ကိုယ့်တစ်ယောက်တည်းဆီမှာပဲထားရမယ့်သော့လို့ မှတ်ထားဖို့လိုပါ တယ်။ အဲဒီသော့နဲ့ မက်ဆေ့ချ်တွေကို ကုဒ်နဲ့ပြောင်းလဲတာရော၊ ပြန်ဖြည်တာ decrypt ရောလုပ်လို့ရပါတယ်။

သော့တွေကိုဘယ်လိုထုတ်လုတ်လဲဆိုတာလေ့လာကြည့်ရအောင်။ အခုဖော်ပြမယ့်နည်းလမ်းက သော့ထုတ်လုပ်တဲ့နေရာမှာ အသုံးများတဲ့ အများသုံးစကားဝှက်သော့နှစ်ချောင်းပါ ဝှက်စာဗေဒဆိုင်ရာကိန်းစဉ်ဖြစ်တဲ့ RSA (Rivest–Shamir–Adleman) နည်းလမ်းဖြစ်ပါတယ်။ RSA ကို PGP သုံး ကုဒ်ဖြင့်ပြောင်းလဲထားတဲ့ အီးမေလ်စနစ်အတွက် သော့အစုံလိုက်ထုတ်ရာမှာ အသုံးပြုပါတယ်။





အများသုံးစကားဝှက်သော့နဲ့ကိုယ်ပိုင်စကားဝှက်သော့ကို အတူထုတ်ပြီးနှစ်ခုလုံးကို ချိတ်ဆက်ထားပါတယ်။ နှစ်မျိုးလုံးက တူညီတဲ့ ကြီးမားတဲ့ကိန်းဂဏန်းတွေကို အခြေခံပြီး လျှို့ဝှက်ထုတ်ထားတာပါ။ ကိုယ်ပိုင်စကားဝှက်သော့က အလွန်ကြီးမားတဲ့ ပြည့်ဝကိန်းဂဏန်းနှစ်ခုကိုကိုယ်စားပြုပြီး အဲဒီကိန်းဂဏန်းနှစ်ခုနဲ့ပဲ အများသုံးစကားဝှက်သော့ ကို ဖန်တီးထားတာပါ။ ထူးခြားတာက အဲဒီကြီးမားတဲ့ပြည့်ဝကိန်းနှစ်ခုက ဘာလဲဆိုတာကို ဖော်ဖို့ အလွန်တရာခက်ခဲတယ်ဆိုတာပါပဲ။

အဲဒီလို ဖော်ထုတ်ဖို့ခက်တဲ့ပြဿနာကို prime factoring လို့ခေါ်ပါတယ်။ အဲ့လို ခန့်မှန်းရခက်တာကို အကြောင်းပြုပြီး အချို့တွေက ကိန်းဂဏန်းကို ခန့်မှန်းတွက်ချက်တဲ့ ကွန်ပျူတာပရိဂရမ်တွေ ထုတ်ခဲ့ပါတယ်။ ဒါပေမဲ့ အခုခေတ်ပေါ်ဝှက်စာဗေဒ cryptography စနစ်တွေမှာတော့ အလွန်တရာကြီးမားလှတဲ့ ပြည့်ဝကိန်းတွေ ကို ကျပန်းရွေးချယ်တဲ့နည်းကိုသုံးထားတာကြောင့် လူတွေအတွက်ရော၊ ကွန်ပျူတာတွေအတွက် ရောဖြေရှင်းဖို့ မလွယ်တော့ပါဘူး။

ဒီစနစ်မှာအားသာချက်တစ်ခုက မိမိတို့ရဲ့ အများသုံးစကားဝှက်သော့ကို မလုံခြုံတဲ့လမ်းကြောင်းတွေကတောင် ပို့ပြီး မက်ဆေ့ချ်တွေကို ကုဒ်နဲ့ပြောင်းလဲပြီးပို့လို့ရအောင်လုပ်ထားတာပါပဲ။ ဒီဖြစ်စဉ်တစ်ခုလုံးမှာ လျှို့ဝှက်ဂဏန်းနှစ်ခုဖြစ်တဲ့ ကိုယ်ပိုင်စကားဝှက်သော့ကို ဘယ်သူ့ဆီမှပို့စရာမလိုဘဲ ကိုယ့်ဆီရောက်လာတဲ့ မက်ဆေ့ချ်တွေကို ပြန်ဖြည်ဖို့သုံးလို့ရတာ အတော်ကောင်းတဲ့အချက်ပါ။

သင့်အနေနဲ့ မှတ်ထားရမှာက အများသုံးစကားဝှက်သော့နှစ်ချောင်းပါဝှက်စာဗေဒအလုပ်ဖြစ်ဖို့ဆိုရင် ပေးပို့သူနဲ့ လက်ခံသူနှစ်ဦးလုံးမှာ တယောက်စီရဲ့ အများသုံးစကားဝှက်သော့တွေရှိနေဖို့ပါ။

အခြားရှုထောင့်ကစဉ်းစားမယ်ဆိုရင် အများသုံးစကားဝှက်သော့နဲ့ ကိုယ်ပိုင်စကားဝှက်သော့တွေကို အတူတကွထုတ်ထားတာ ဖြစ်ပြီး ရင်နဲ့ရန်လိုနှစ်ခုလုံးက ချိတ်ဆက်နေတယ်ဆိုတာပါပဲ။

သင့်အများသုံးစကားဝှက်သော့ကို လူအများက ရှာဖွေလို့ရသလို၊
လူအများဆီဖြန့်ဝေထားလို့လည်းရပါတယ်။ ဘယ်သူ့ဆီကိုမဆိုပေးထားလို့ရပါတယ်။
သင့်အီးမေးလ်လိပ်စာကို တခြားသူ သိသွားမှာ ဝန်မလေးဘူး ဆိုရင်
သင့်ဆိုရှယ်မီဒီယာမှာလည်းတင်ထားလို့ရပါတယ်။ သင့်ရဲ့ကိုယ်ပိုင်ဝက်ဘက်ဆိုက်မှာလည်းတင်
လို့ရပါတယ်။ သင်ပေးချင်သလိုပေးလို့ရပါတယ်။

ဒါပေမဲ့ကိုယ်ပိုင်စကားဝှက်သော့ကိုတော့ သင်နဲ့နီးရာမှာလုံခြုံစွာသိမ်းပါ။
သင့်မှာအဲဒီတစ်ချောင်းပဲရှိတာမို့ ပျောက်လို့မရပါဘူး။ သူများကို ပေးလို့လည်းမရပါဘူး။
ပုံတူပွားပြီးလျှောက်ဖြန့်လို့လည်း မရပါဘူး။ မဟုတ်ရင် သင့်ကိုယ်ပိုင်မက်ဆေ့ချ်တွေက
သင့်ကိုယ်ပိုင်မဟုတ်တော့ဘဲ ဖြစ်သွားပါလိမ့်မယ်။

PGP ဘယ်လိုအလုပ်လုပ်သလဲ

ဒီ PGP ဥပမာကိုကြည့်ပြီး အများသုံးစကားဝှက်သော့ပါ ဝှက်စာဗေဒဘယ်လိုအလုပ်လုပ်သလဲဆိုတာ
ကြည့်ရအောင်။ သင့်အနေနဲ့ အာရဗ်ဆီ လျှို့ဝှက်မက်ဆေ့ချ်ပို့ချင်တယ်ဆိုပါစို့။

> (၁) အာရဗ်ဆီမှာ ကိုယ်ပိုင်စကားဝှက်သော့တစ်ချောင်းရှိမယ်။ သူက
> အများသုံးစကားဝှက်သော့ဖြင့် ကုဒ်ပြောင်းလဲ ခြင်း စနစ်ကို
> ကျွမ်းကျွမ်းကျင်ကျင်သုံးတတ်တဲ့အတွက် သူ့ဆီမှာရှိတဲ့ အများသုံးစကားဝှက်သော့ကို (HTTPS
>) ဝက်ပေ့ချ်မှာတင်ထားမယ်။

(၂) သင်ကသူ့ရဲ့ အများသုံးစကားဝှက်သော့ကို ဒေါင်းလုတ်ဆွဲမယ်။

(၃) သူ့ရဲ့အများသုံးစကားဝှက်သော့ကိုသုံးပြီး သင်ကလျှို့ဝှက်မက်ဆေ့ချ်ရေးမယ်။ သူ့ဆီပို့မယ်။

(၄) သင်ပို့တဲ့မက်ဆေ့ချ်ကို အာရဗ်ကပဲ ပြန်ဖြည်နိုင်မှာဖြစ်တယ်။ ဘာလို့လဲဆိုတော့ သူ့ဆီမှာပဲ အများသုံးစကားဝှက်သော့နဲ့ချိတ်ဆက်ထားတဲ့ ကိုယ်ပိုင်စကားဝှက်သော့ရှိလို့ပါ။

Pretty Good Privacy (PGP) က အများသုံးစကားဝှက်သော့နဲ့ ကိုယ်ပိုင်စကားဝှက်သော့တွေကို တိကျစွာ ထုတ်လုပ် အသုံးပြုနိုင်ဖို့ ဖန်တီးထားတာပါ။ PGP ကိုသုံးပြီး အများသုံးနဲ့ကိုယ်ပိုင်စကားဝှက်သော့တစ်စုံကို ဖန်တီးနိုင်ပါ တယ်။ ထွက်လာတဲ့ ကိုယ်ပိုင်စကားဝှက်သော့ကို password စကားဝှက်နဲ့ လုံခြုံစွာသိမ်းပြီးသုံးလို့ရတယ်။ အများသုံးစကားဝှက်သော့ကိုတော့လက်မှတ်ထိုးဖို့နဲ့ စာတွေကိုကုဒ်နဲ့ပြောင်းဖို့အသုံးပြုနိုင်ပါတယ်။

ဒီအပိုင်းမှာအဓိကမှတ်သားထားစေလိုတဲ့အချက်ကတော့ သင့်ရဲ့ကိုယ်ပိုင်စကားဝှက်သော့ကို လုံခြုံတဲ့နေရာမှာ ဝှက်စာကြောင်းအရှည်ကြီး passphrase နဲ့ သေသေချာချာသိမ်းထားဖို့ပါ။

အချက်အလက်များအကြောင်းရှင်းပြသည့်အချက်အလက်များ နှင့် အများသုံးစကားဝှက်သော့ဖြင့် ကုဒ်ပြောင်းလဲခြင်းက ဘာတွေလုပ်မပေးနိုင်ဘူးလဲ။

အများသုံးစကားဝှက်သော့ဖြင့် ကုဒ်ပြောင်းလဲခြင်းရဲ့ အဓိကလုပ်ဆောင်ချက်က ပို့လိုက်တဲ့ မက်ဆေ့ချ်တွေမှာပါဝင်တဲ့ အကြောင်းအရာတွေရဲ့လုံခြုံမှုနဲ့ ဘယ်သူကမှကြားဖြတ်ခိုးယူပြောင်းလဲလို့ မရစေဖို့ဖြစ်ပါတယ်။ ကိုယ်ရေးလုံခြုံမှုက ဒါ့ထက်ပိုပါတယ်။ အထူးသဖြင့် သင့်မက်ဆေ့ချ်တွေ အကြောင်းရှင်းပြတဲ့ အချက်အလက်တွေ (See “metadata”)ကလည်း မက်ဆေ့ချ်မှာပါတဲ့ အကြောင်းအရာတွေနည်းတူ အရေးကြီးပါတယ်။

သင့်အနေနဲ့ သင့်နိုင်ငံမှာရှိတဲ့နာမည်ကျော်အတိုက်အခံနဲ့ လျှို့ဝှက်မက်ဆေ့ချ်တွေအပြန်အလှန် ပို့နေတယ်ဆိုရင် သင့်အတွက် အန္တရာယ်ရှိပါတယ်။ မက်ဆေ့ချ်တွေကို ပြန်ဖြည်လို့မရစေဦးတော့ သူနဲ့ အဆက်အသွယ်ရှိတယ်ဆိုတာကိုက အန္တရာယ်ဖြစ်နေပြီလေ။ အချို့နိုင်ငံတွေမှာဆိုရင် ကုဒ်နဲ့ ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ်တွေကိုပြန်ဖြည်ဖို့ အမိန့်ကိုငြင်းဆန်တာနဲ့ ထောင်ဒဏ်သင့်တာမျိုးအထိ ဖြစ်နိုင်ပါတယ်။

အများသိလို့မရတဲ့လူနဲ့ဆက်သွယ်တဲ့အခါ အခြားသူတစ်ယောက်နဲ့ဆက်သွယ်တဲ့ပုံစံမျိုးဖြစ်အောင် လုပ်ယူတာပိုခက်ပါတယ်။ PGP နည်းလမ်းကောင်းတစ်ခုကတော့ အမည်မဖော်ထားတဲ့ လျှို့ဝှက်အီးမေးလ်အကောင့်တွေသုံးဖို့နဲ့ ချိတ်ဆက်မှုတွေကို Tor ကတဆင့်လုပ်ဖို့ပါ။ အဲဒီလိုလုပ်တဲ့အတွက် PGP ကို ဆက်သုံးလို့ရပါမယ်။ သင်တို့က အခြားသူတွေမသိတဲ့ သီးခြားအီးမေးလ်တွေ သုံးပြီး ဆက်သွယ်တာမို့ အခြားသူတွေဆီက အယောင်ဆောင်အီးမေလ်းတွေရဖို့ခက်သွားစေပါလိမ့်မယ်။ သင်တို့အချင်းချင်းပို့တဲ့အီးမေးလ်တွေဖြစ်ကြောင်းအတည်ပြုဖို့လွယ်သွားတာပေါ့။

သင့်အနေနဲ့ အများသုံးစကားဝှက်ကုဒ်ဖြင့်ပြောင်းလဲခြင်းအကြောင်း အတော်လေးသိသွားပြီဖြစ်တဲ့အတွက် end-to-end encryption အက်ပ်ဖြစ်တဲ့ Signal for iOS (သို့မဟုတ်) Android ကိုစမ်းသုံးကြည့်ပါ။