RockYou के लीक हुए पासवर्ड का संक्षिप्त विश्लेषण

पास्केप सोफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)

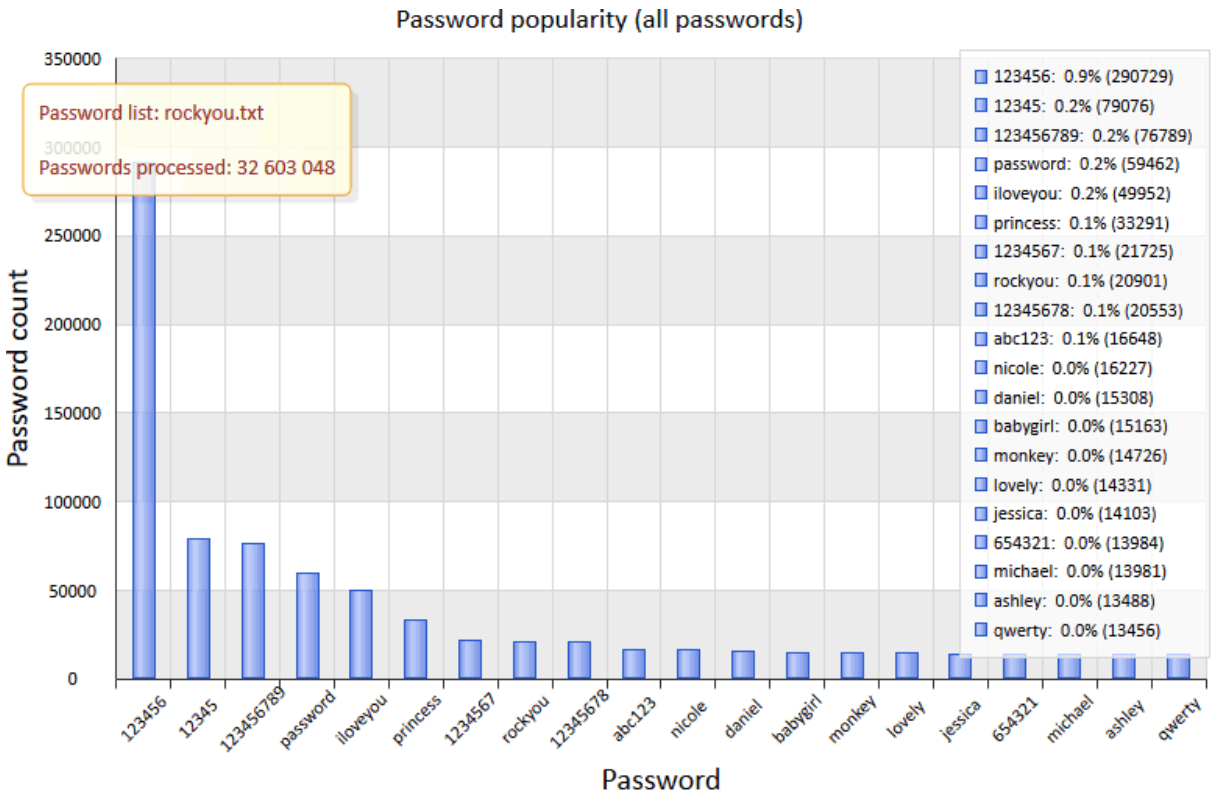
RockYou के लीक हुए पासवर्ड का संक्षिप्त विश्लेषण

1 RockYou के लीक हुए पासवर्ड का संक्षिप्त विश्लेषण

1.1 सार

दिसंबर 2009 में RockYou.com वेबसाइट पर हैकर्स ने हमला किया था। हमला सफल रहा और इसके परिणामस्वरूप वेबसाइट के यूजर्स के 32.6 मिलियन चुराए गए पासवर्ड वाले टेक्स्ट डेटाबेस का अवैध खुलासा हुआ। गोपनीय डेटा के इस बड़े रिसाव ने हमें यह देखने की अनुमति दी है कि लोग अपने पासवर्ड कैसे बनाते हैं और बाहरी पर्यवेक्षक के दृष्टिकोण से एक बहुत ही सरल सुरक्षा ऑडिट करने के लिए। सांख्यिकीय डेटा एकत्र और संसाधित करने के लिए, हमने विंडोज पासवर्ड रिकवरी टूल का उपयोग किया।

1.2 टॉप 20 लोकप्रिय पासवर्ड

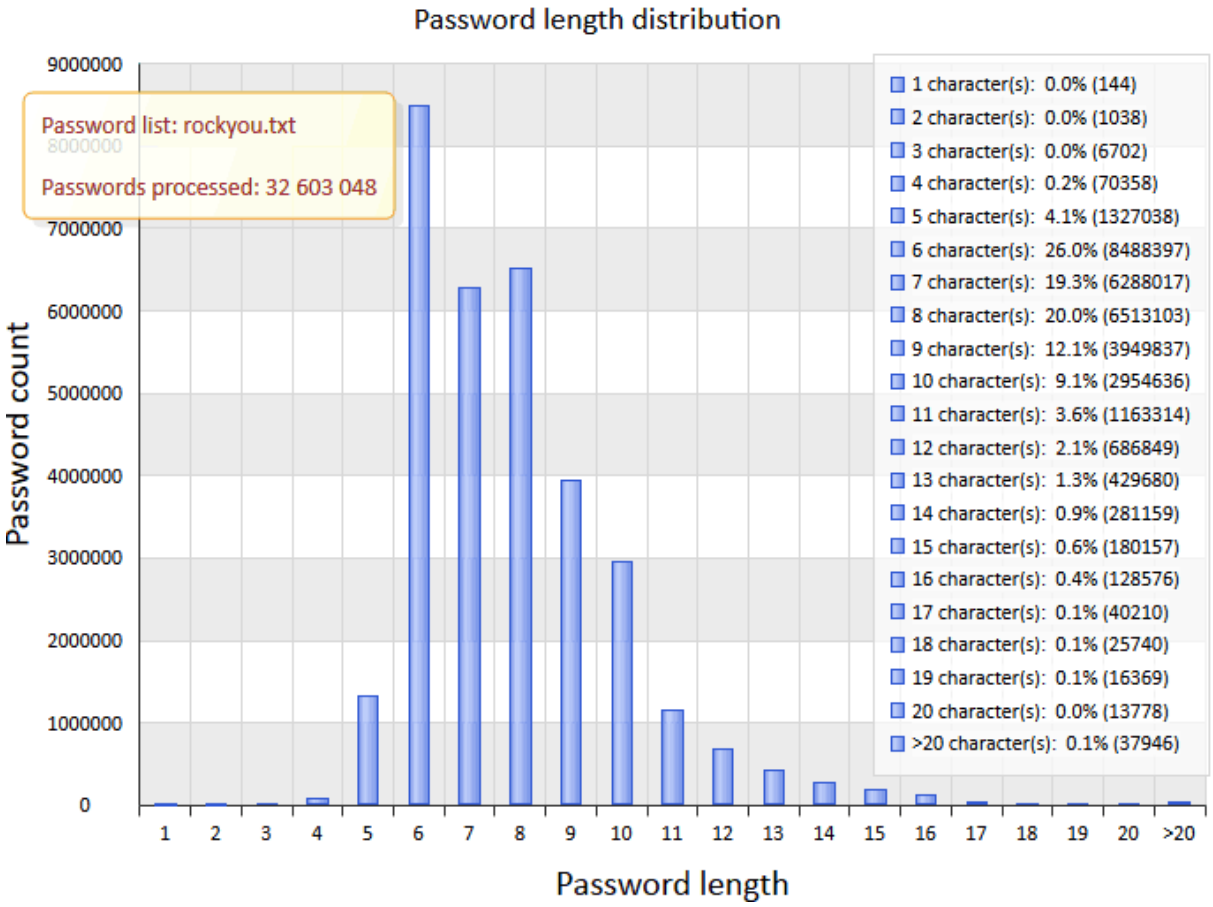


सबसे लोकप्रिय पासवर्डों में से "**123**" से अधिक जटिल कुछ खोजना कठिन है, इसलिए टॉप 20 बिल्कुल भी आश्चर्यजनक नहीं है। जैसा कि आप देख सकते हैं, सबसे लोकप्रिय पासवर्ड ("**123456**") पैक से बहुत आगे है। इसकी लोकप्रियता संख्या में भी आश्चर्यजनक है: 32 मिलियन रिकॉर्ड में से 290,000। हमारे एक सहयोगी ने सुझाव दिया कि जिस डेटाबेस में 10 सबसे लोकप्रिय पासवर्ड 1 प्रतिशत से अधिक रिकॉर्ड की गणना करते हैं, उसे असुरक्षित माना जाना चाहिए। RockYou.com डेटाबेस में, यह "असुरक्षा कारक" 2 गुना से अधिक है। लोकप्रिय पासवर्ड का विश्लेषण करते समय, हमने उन्हें सामान्य विशेषताओं के आधार पर कई समूहों में वर्गीकृत किया:

- **डिक्शनरी पासवर्ड**, यही है, "password," "monkey" और इसी तरह के शब्द, सबसे स्थिर समूहों में से एक बनाते हैं।
- **डिजिटल पासवर्ड** आसानी से याद किए जाने वाले संख्यात्मक संयोजनों के आधार पर, फ़ोन नंबर, दस्तावेज़ संख्या, जन्म तिथि, और बहुत कुछ एक और समूह बनाते हैं, जो पिछले वाले की तरह स्थिर है, और शायद और भी अधिक लोकप्रिय है।

- **नामों के आधार पर पासवर्ड** और उनके डेरिवेटिव। उदाहरण के लिए, कोई यूजर अपने नाम, अपने पालतू जानवर, किसी शहर, किसी स्थान आदि का उपयोग कर सकता है।
- **कीबोर्ड संयोजनों पर आधारित** पासवर्ड, जैसे "abc123," "qwerty" आदि।
- **भावनात्मक पासवर्ड**, जैसे "iloveyou", "hateu" "lovely", "ihatmyboss" या "ILoveJohn"।

1.3 पासवर्ड लंबाई वितरण



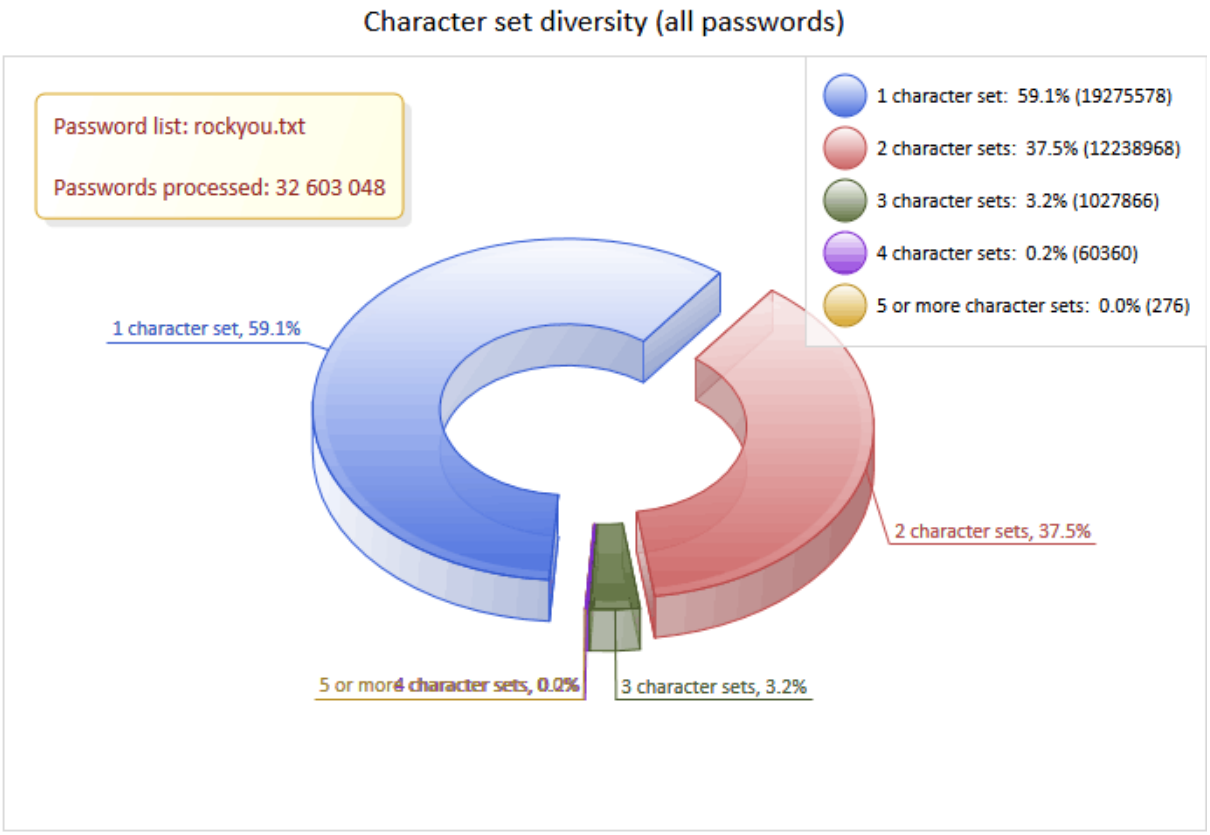
एक पासवर्ड की लंबाई हमलों के खिलाफ उसके प्रतिरोध का एक महत्वपूर्ण फेक्टर है। आप कह सकते हैं कि पासवर्ड जितना लंबा होगा, उसे तोड़ना उतना ही कठिन होगा। लेकिन यह मत भूलो कि यह अस्थिर संतुलन आसानी से खो सकता है यदि यूजर द्वारा बहुत सारे पेय के साथ एक जीवंत पार्टी के बाद लंबे पासवर्ड को "सफलतापूर्वक" भुला दिया जाता है। कुछ यूजर पासवर्ड के साथ स्टिकी नोट्स सीधे अपने मॉनिटर पर डालते हैं, लेकिन अधिकांश कम परिष्कृत होते हैं और अधिक से अधिक 7 या 8 वर्णों वाले आसानी से याद किए जाने वाले पासवर्ड पसंद करते हैं।

जैसा कि आप चार्ट पर देख सकते हैं, सबसे लोकप्रिय पासवर्ड **6, 8, या 7** वर्णों की लंबाई के होते हैं। यह सभी पासवर्डों का **65** प्रतिशत से अधिक है। इसका मतलब है कि 3 में से 2 पासवर्ड आसानी से ब्रूट-फ़ोर्स हो सकते हैं।

उत्सुकता से पर्याप्त, कुछ यूजर्स 20 से अधिक वर्णों, शब्द संयोजनों या वाक्यांशों से युक्त अश्लील रूप से लंबे पासवर्ड चुनते हैं। यहां कुछ अद्भुत पासवर्ड दिए गए हैं (क्या आपने वास्तव में सोचा था कि कोई नहीं जानता कि आप क्या टाइप कर रहे हैं?):

Hahaithinkilovejessebutthenagainmaybenotcuzheisadiknob
Lets you come back for your Countdown Timer
me plus food equals more sleep each night
tommmmmmmmmmmmmmmmmmmmmmmmm
truongcaodangcongdonghaiphong
icantbelievethisshit.12345
banditbanditbandit1bandit1bandit1banditbandit
111111111111111111111111111111111111111111
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
FUCKSCHOOLANDALLTHETEACHERSINIT
ilovepalmermyfuturehusband
1delightyourselfinthelord!
Imaprincessbecausemyfatheristheking
iluvanjabisset4evashesmawebaexxx
stuartandchrisrmybestmatesforeva
thisismypasswordyoullnevergetit

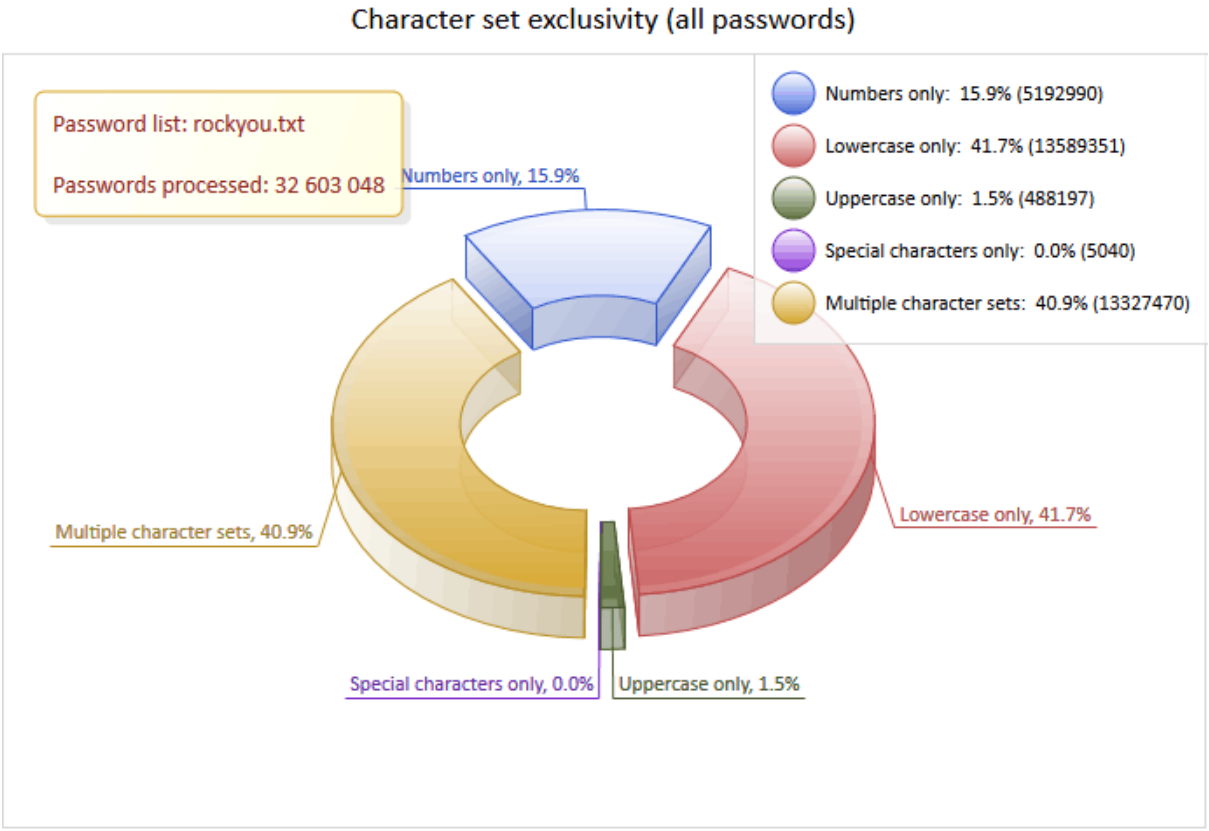
1.4 कैरेक्टर सेट विविधता



पासवर्ड की ताकत को प्रभावित करने वाला एक अन्य महत्वपूर्ण फेक्टर वर्णों की विविधता है। उदाहरण के लिए, 7-वर्ण पासवर्ड "**aB1~cde**" 9-वर्ण पासवर्ड "**abcdefghi**" से 10 गुना अधिक मजबूत है।

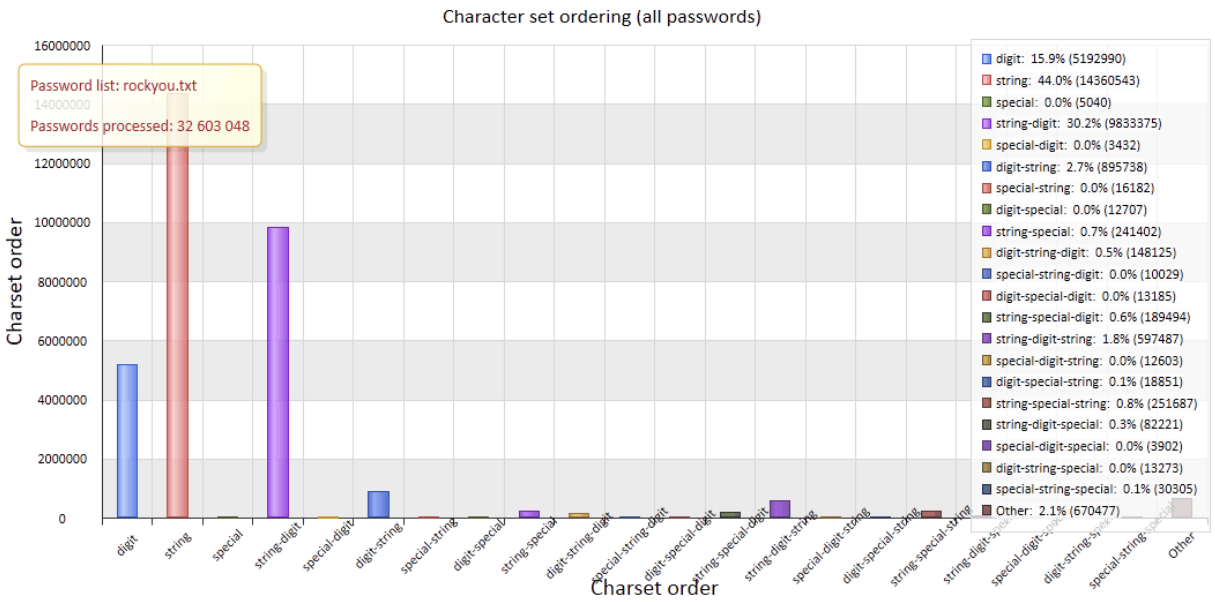
आधे से अधिक यूजर्स के पासवर्ड में केवल एक वर्ण सेट होता है। उदाहरण के लिए, वे केवल अंकों या केवल छोटे अक्षरों का उपयोग करते हैं। 96.5 प्रतिशत से अधिक यूजर्स के पास केवल एक या दो वर्ण सेट हैं, और 3.5 प्रतिशत से कम तीन या अधिक वर्ण सेट का उपयोग करते हैं। पासवर्ड की लंबाई और विविधता के चार्ट स्पष्ट रूप से दिखाते हैं कि पासवर्ड चुनने में यूजर्स की प्राथमिकताएं पिछले दो दशकों में मुश्किल से बदली हैं। हमारा निष्कर्ष: हमने इस मिथक को सफलतापूर्वक खारिज कर दिया है कि आप यूजर्स को मजबूत पासवर्ड (कम से कम, इस मामले में) का उपयोग करने के लिए मजबूर कर सकते हैं।

1.5 कैरेक्टर सेट चुनने में वरीयता



सामान्य आंकड़े बताते हैं कि एक वर्ण सेट के आधार पर पासवर्ड चुनते समय, यूजर ज्यादातर केवल लोअर-केस अक्षरों (सभी पासवर्डों के 41 प्रतिशत से अधिक), केवल अंकों (लगभग 16 प्रतिशत), या अपर-केस अक्षरों वाले शब्दों को पसंद करते हैं। (1.5 प्रतिशत)। केवल विशेष वर्णों वाले पासवर्ड का उपयोग बहुत ही कम किया जाता है।

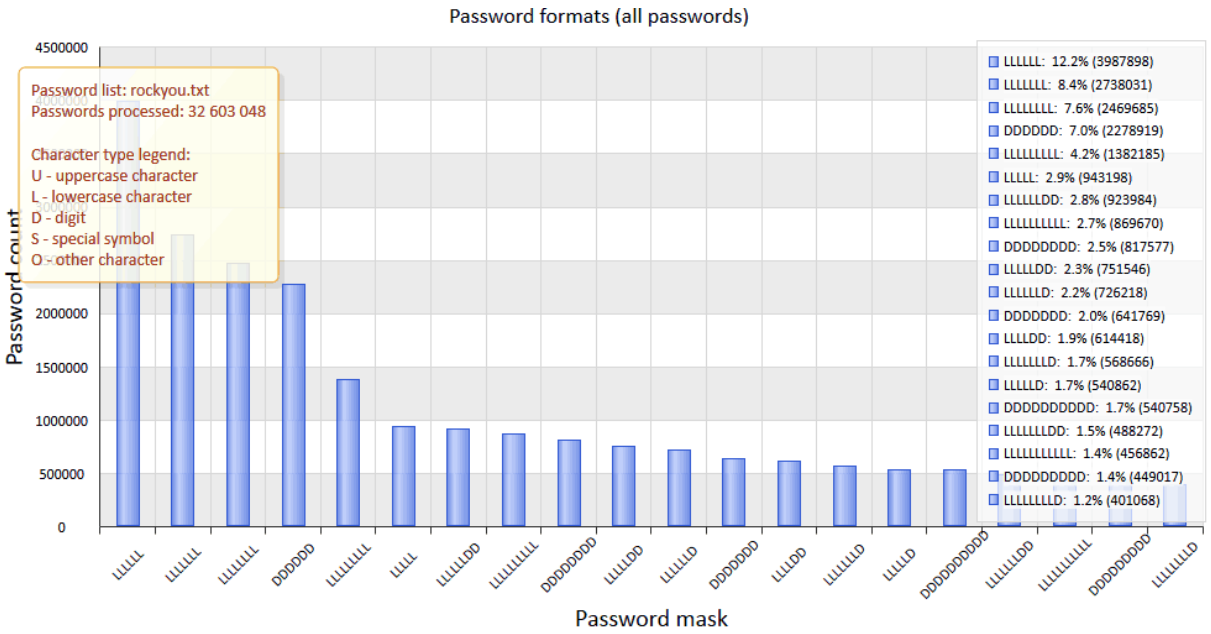
1.6 पासवर्ड में कैरेक्टर सेट ऑर्डर



यदि आप इस चार्ट पर एक नज़र डालते हैं, तो आप इस तथ्य पर आश्चर्यचकित हो सकते हैं कि दो या दो से अधिक वर्ण सेट वाले अधिकांश पासवर्ड **स्ट्रिंग-अंक** या **अंक-स्ट्रिंग** संयोजन होते हैं। सोशल इंजीनियरिंग में कुशल एक हमलावर इस तरह के पासवर्ड को क्रैक करने के लिए इस अवलोकन का उपयोग कर सकता है।

हमारा निष्कर्ष: "**iloveyou12345**" पासवर्ड "**iloveyou**" पासवर्ड जितना ही कमजोर है।

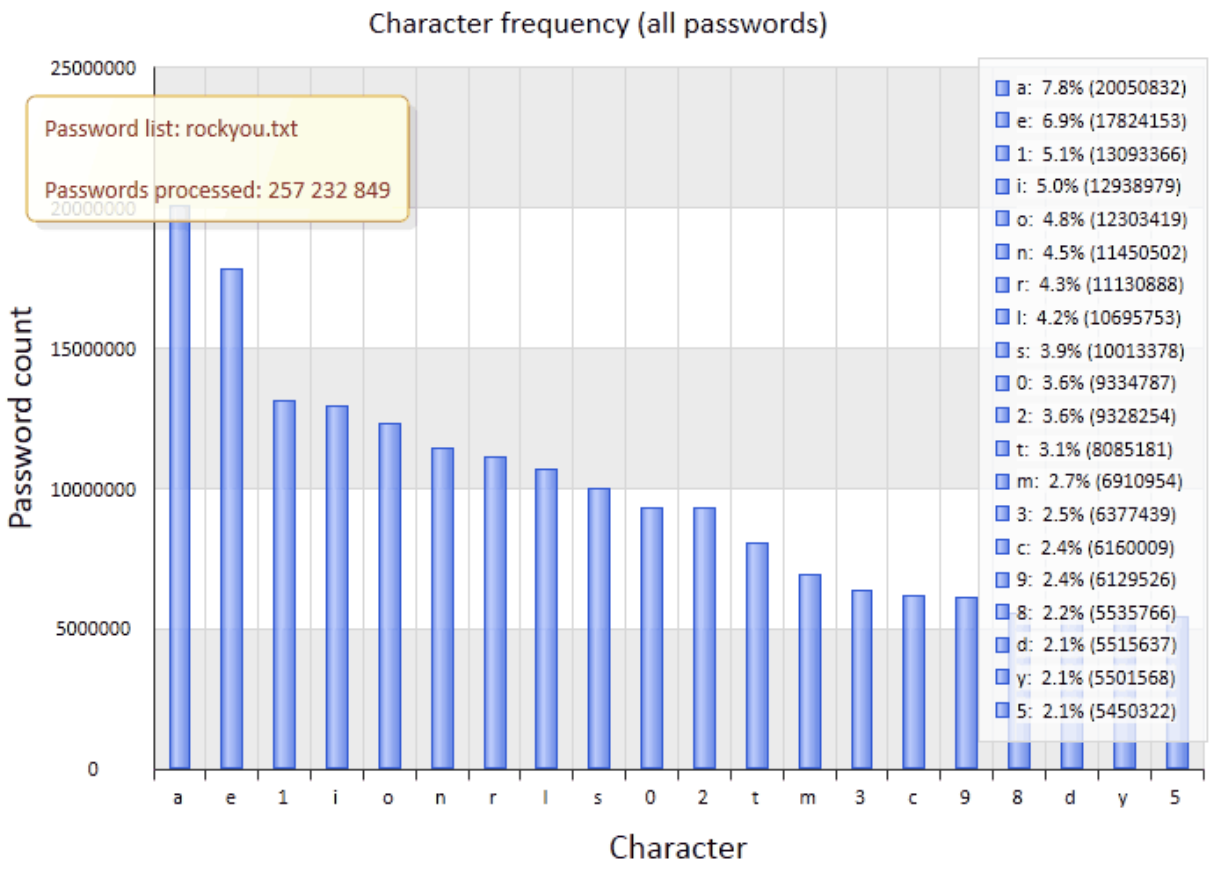
1.7 पासवर्ड प्रारूप



अब आइए पासवर्ड मास्क, कैरेक्टर बाय कैरेक्टर पर विचार करें। सबसे लोकप्रिय पासवर्ड में 6, 7, या 8 वर्ण होते हैं और केवल एक वर्ण सेट का उपयोग करते हैं। अनुमान लगाया जा सकता है, है ना? अधिक परिष्कृत पासवर्ड में, यूजर आमतौर पर एक या एक से अधिक अंक एक शब्द के अंत में लगाते हैं।

हमारा निष्कर्ष: पासवर्ड अनुमान लगाने की प्रक्रिया को तेज करने के लिए, एक हमलावर पासवर्ड प्रारूपों का एक बहुत ही सरल विश्लेषण कर सकता है और विशेष टेम्पलेट (मास्क) बना सकता है।

1.8 कैरेक्टर फ़्रीक्वेंसी



यह कैरेक्टर फ़्रीक्वेंसी चार्ट पासवर्ड सूची में सबसे अधिक बार उपयोग किए जाने वाले वर्णों को दिखाता है। इसके अलावा, इन आँकड़ों का उपयोग गणितीय विश्लेषण के लिए किया जा सकता है, जैसे मार्कोव श्रृंखलाओं का निर्माण। आप सोच सकते हैं कि ऐसे आँकड़े बिलकुल बेकार हैं, है ना? काश, ऐसा नहीं होता। यदि आप सबसे अधिक उपयोग किए जाने वाले २० वर्णों वाले किसी भी पासवर्ड के लिए Rockyou.txt में सभी रिकॉर्ड का विश्लेषण करते हैं, तो आप पाएंगे कि डेटाबेस में उनमें से 4,789,597 या कुल संख्या का 14.7 प्रतिशत हैं। सिद्धांत रूप में, इस तरह के विश्लेषण का उपयोग पासवर्ड के बेहतर और तेज़ ब्रूट-फोर्सिंग के लिए सही वर्ण सेट बनाने के लिए किया जा सकता है।

1.9 निष्कर्ष

हाल ही में हम एक बहुत ही चिंताजनक प्रवृत्ति देख रहे हैं: मूर के नियम का पालन करते हुए आज के कंप्यूटरों का प्रदर्शन लगातार बढ़ रहा है, और पासवर्ड ब्रूट-फोर्सिंग के लिए ग्राफिक्स प्रोसेसर (जीपीयू) का उपयोग करने का अवसर और भी अधिक खतरनाक है। यहां तक कि एक लो-एंड क्वाड-कोर सीपीयू प्रति सेकंड 100,000,000 से अधिक विंडोज एनटी पासवर्ड की जांच कर सकता है, और एक सस्ते जीपीयू का प्रदर्शन परिमाण का एक क्रम है। उदाहरण के लिए, GPU का उपयोग करने से आप कुछ ही सेकंड में 7-वर्णों के पासवर्ड को ब्रूट-फ़ोर्स कर सकते हैं! ऐसा लगता है कि सॉफ़्टवेयर

विक्रेताओं को वैकल्पिक डेटा सुरक्षा विधियों को खोजना होगा या पासवर्ड-संरक्षित सिस्टम में एन्क्रिप्शन एल्गोरिदम को अप-टू-डेट रखना होगा।

सरल पासवर्ड क्रैकिंग विधियों, जैसे कि ब्रूट-फोर्सिंग या डिक्शनरी सर्च, को सांख्यिकीय प्रसंस्करण, गणितीय विश्लेषण, टेम्प्लेट, सोशल इंजीनियरिंग, नए प्रकार के हमलों आदि के आधार पर अधिक उन्नत टूल द्वारा प्रतिस्थापित किया जा रहा है।

उपरोक्त आश्चर्यजनक नहीं होना चाहिए। एक प्राचीन यूनानी ने कहा था कि हमारे आस-पास की दुनिया में (मनुष्य की मूर्खता को छोड़कर) कुछ भी एक जैसा नहीं रहता। यहां उनके कथन का हमारा वर्जन है: कुछ भी समान नहीं रहता है, लेकिन लोगों की अपनी सुरक्षा के प्रति लापरवाह दृष्टिकोण सामान है। यदि आप मेरा अनुसरण करते हैं, तो एक मजबूत पासवर्ड "123456" या "qwerty" जैसी किसी चीज़ से बहुत बेहतर है यदि आप इसे अपनी नोटबुक में या पोस्ट-इट नोट पर लिखते हैं (भले ही आप इसे अपने मॉनिटर पर चिपका दें)। सामान्य युजर्स को अपनी सुरक्षा के बारे में अधिक परवाह करना मुश्किल है क्योंकि उनके दिमाग में पहले से ही बहुत सी अन्य समस्याएं हैं। इसलिए सॉफ्टवेयर विक्रेताओं को इसे यूजर का बोझ बनाकर नहीं बल्कि अपने उत्पादों में अधिक उन्नत पासवर्ड सुरक्षा एल्गोरिदम विकसित और कार्यान्वित करके बेहतर सुरक्षा प्रदान करनी चाहिए जो आज की जरूरतों को बेहतर ढंग से पूरा करते हैं।