این الگوریتم توسط اداره استانداردها و فناوری های مدرن آمریکا جهت استفاده عموم بوجود آمد . این الگوریتم در سال ۱۹۹۳ معرفی شد و جایگزین مناسبی برای MD5 بود . مهم تر آن که عنوان استاندارد دولت فدرال آمریکا را با خود یدک می کشید . البته این روش هم در سال ۲۰۰۵ در هم کوبیده شد .

این روش مانند MD5 است با این تفاوت که طول چکیده پیام ۲۰ بایت می باشد .این روش هم مانند MD5 از or و حلقه های تکرار استفاده می کند .

این الگوریتم در بسیاری از محصولات سخت افزاری و نرم افزاری به کار گرفته شده بود ، در واقع SHA -1 نسخه ارتقا یافته ای از SHA-0 بود که در سال ۱۹۹۳ توسط بیهام در هم کوبیده شده بود . بسیاری از رمزشکن هامعتقد بودند SHA-1 هم به دلیل شباهت به SHA-0 قابل شکستن است و برای مقابله با این ایده سازمان استاندارد آمریکا سریعا نسخه های SHA-256,SHA-512 را معرفی کرد ولی نهایتا برخورد در SHA-1 در سال ۲۰۰۵ و توسط گروهی چینی به سرپرستی ژیایون ونگ شناسایی شد و درستی این ادعا توسط بروس شاینر از بزرگان رمزنگاری جهان اثبات شد و نهایتا برخوردی در سال ۲۰۰۶ رسما ثبت گردید .

از آن جا که پیچیدگی در این الگوریتم دو به توان شصت ونه اعلام شده بود هنوز اندک امیدی باقی بود که در مدت ۶ ماه روش جایگزینی اعلام شود .