AI Starts Finding Cracks in Old Cryptography, Gemini Omni Edits Video by Conversation, and Chatbots Reach for Your Bank Data

Google DeepMind reportedly says AI-guided analysis exposed two weaknesses in legacy 1024-bit RSA, Google's Gemini Omni Flash brings talk-to-edit video to the mainstream, and Anthropic's leaked Personal Finance feature shows how read-only guardrails are becoming the template for agents near money.

Themes: Governance & Safety · Models & Frontier

Note: web page fetches were blocked today, so this lesson relies on search-result summaries from news and aggregator sites. Dates, figures and product names are secondary reports and unverified; check the original announcements.

1) AI as a Codebreaker: Weaknesses in Legacy 1024-bit RSA

Newsletter coverage dated November 6, 2026 says Google DeepMind announced that AI models, guided by human cryptanalysis experts, uncovered two significant weaknesses in legacy 1024-bit RSA cryptosystems within weeks. My searches could not confirm a primary DeepMind post. Related, verifiable context: a September 22 paper from UC San Diego and INRIA showed practical signature forgery against deprecated 1024-bit RSA keys without factoring the private key, while stating that widely used modern RSA implementations remain safe. A Cloud Security Alliance research note from October 2026 also discusses an 'assumption horizon' for AI-assisted cryptanalysis.

The concept, explained simply: Public-key encryption such as RSA rests on a bet: some maths problems (like splitting a huge number into its prime factors) are too slow to solve. Cryptanalysis is the hunt for shortcuts. An AI helps like a tireless junior researcher: it tries thousands of algebraic patterns and proposes candidate shortcuts, and human experts check which ones are real. 1024-bit keys are 'legacy' because the standard advice is already 2048 bits or more.

Why it matters: Cryptography's security is only as good as the shortest known attack. If AI speeds up the search for attacks, the safe lifetime of older keys shrinks. The practical lesson is hygiene rather than panic: find and retire 1024-bit keys, move to 2048+ bits, and plan the move to post-quantum algorithms, since AI and quantum progress both erode today's assumptions.

2) Gemini Omni Flash: Edit Video by Talking to It

Google introduced Gemini Omni Flash at I/O on May 19, 2026, a model that generates short video with synchronized audio from text, image, audio or video inputs and lets you refine the result in conversation. It rolled out in the Gemini app, Google Flow and YouTube Shorts, with free access through Shorts and paid access from about $7.99 a month. A digest this week reports a Gemini Omni 1.2 Flash general-availability release with 15-second clips, conversational editing and roughly 30% lower cost; I could not confirm the '1.2' naming or those figures from primary sources. All outputs carry Google's SynthID watermark.

The concept, explained simply: Older video generators worked like a vending machine: type a prompt, get a clip, start over if you dislike it. A conversational model keeps the clip in memory, so you say 'make the sky sunset-orange and slow the camera' and only those parts change. It is the difference between re-ordering a whole meal and asking the chef to adjust one dish.

Why it matters: Editing by instruction lowers the skill barrier for video, which is why distribution through YouTube Shorts matters more than the benchmark. It also raises provenance stakes: watermarks like SynthID let platforms and viewers check whether a clip is AI-made, and that verification becomes part of the product.

3) Agents Near Your Money: Read-Only by Design

Reports this week say Anthropic is preparing a Personal Finance feature for Claude (earlier leaked as 'Claude Money'), linking bank accounts through Plaid with onboarding screens promising read-only access. Anthropic had not publicly confirmed a launch, date, pricing or supported banks as of the latest coverage I could find, and a US-first release is only an expectation. Separately, Claude was reported to add native OpenTelemetry export to Databricks MLflow, giving teams traces for debugging agent behaviour. OpenAI's own finance product is described as read-only too: it cannot move money, pay bills or trade.

The concept, explained simply: Read-only access means the agent can look at your balances and transactions to explain them, spot unusual spending or build a budget, but it has no ability to send money or change settings. Pair that with tracing (logging every step an agent takes) and you have two layers: limited power, plus a record you can audit.

Why it matters: Finance is the highest-trust domain for consumer agents. A leak of bank data or a wrong transfer is costly, so labs start with the narrowest permission that is still useful. This echoes last week's consent gates: the pattern for 2026 agents is least privilege first, then widen access as reliability is proven.

VIRAL / OPEN-SOURCE SPOTLIGHT

Gemini Omni Flash (Google): A video model that turns a text, image or audio prompt into a short clip with sound, then lets you edit it by chatting ('make it slower, add rain'). It is taking off because it is free inside YouTube Shorts for ordinary creators, needs no editing skills, and arrives with a built-in watermark. Limits to know: clips are only seconds long, quality varies, and I could not verify usage numbers or the reported newer 1.2 version. Try it by taking one photo and asking for a five-second clip, then change a single element through follow-up messages.

MARKET SIGNAL

Capital keeps flowing to the frontier: a report this week says OpenAI raised $11 billion at a $1.25 trillion valuation, while Anthropic's revised IPO filing reportedly says its internal estimates show it may 'imminently meet' its policy's definition of dramatically accelerated, AI-driven progress. Meanwhile, cyber capability is now a headline metric, with one report claiming an OpenAI cyber model found 948 Linux kernel exploits. Expect valuations, security capability and consumer distribution to be the competitive axes. All figures are unverified secondary reports.

PRACTICAL TAKEAWAYS

1) Audit for 1024-bit keys.
Inventory certificates, SSH keys and signing keys now and replace anything under 2048 bits.

2) Start post-quantum planning.
AI-aided cryptanalysis and quantum advances both shorten legacy key lifetimes, so map where you depend on RSA.

3) Edit video by iterating, not restarting.
Give one change per follow-up message so a conversational video model keeps the parts you liked.

4) Check provenance on AI video.
Use SynthID-style verification before sharing or trusting a clip, and label your own AI-made content.

5) Give finance agents read-only access first.
Connect accounts without transfer rights and require logs or traces before widening permissions.

SELF-TEST

Q1. Why is a 1024-bit RSA key called legacy?

A1. Current guidance is 2048 bits or more, and shorter keys have a shrinking safety margin against better attacks.

Q2. How does an AI help in cryptanalysis?

A2. It searches many candidate patterns and proposes shortcuts that human experts then verify.

Q3. What makes conversational video editing different from prompt-only generation?

A3. The model keeps the clip in context, so follow-up instructions change only the requested parts.

Q4. What does read-only access mean for a finance agent?

A4. It can view balances and transactions to analyse them but cannot move money or change settings.

TOMORROW

What We're Watching: a primary DeepMind publication detailing the RSA findings and which key sizes are affected. What We're Watching: whether Anthropic officially announces Personal Finance and its permission model. What We're Watching: confirmation of the Gemini Omni 1.2 Flash release and its pricing. What We're Watching: independent verification of the reported funding and exploit-count figures.

TOPICS COVERED SO FAR (RECAP)

Recent days covered the cheap fast model tier (GPT-6.1 Terra), the Agent Client Protocol in Android Studio, compute commitments in Anthropic's amended S-1, always-on Dots agents, staged model release and agent monitoring, agent swarms, Chrome DevTools MCP, proactive agents (Claude Duet, Meta Muse), mixture-of-experts open-weight models (Kimi K3.1 Pro) and consent gates. Today added AI-assisted cryptanalysis of legacy RSA, conversational video editing with Gemini Omni Flash, and read-only guardrails for finance agents.

Sources: solutionsreview.com, aisdg.substack.com, theneuron.ai, dev.to (daily digests for Nov 6-7, 2026); labs.cloudsecurityalliance.org and scworld.com (AI cryptanalysis context); phonearena.com, officechai.com and wavespeed.ai (Gemini Omni Flash); fourweekmba.com, testingcatalog.com, techrepublic.com and bleepingcomputer.com (Claude Personal Finance). Figures are secondary reports and unverified.